ANEXO 1

PLANEJAMENTO ESTRATÉGICO 2015 - 2018

Instituto Nacional de Tecnologia da Informação

Planejamento Estratégico 2015-2018

Instituto Nacional de Tecnologia da Informação

Autarquia vinculada à Casa Civil da Presidência da República

Diretor-Presidente

Renato da Silveira Martini

Diretor de Infraestrutura de Chaves Públicas – DINFRA

Maurício Augusto Coelho

Diretor de Auditoria, Fiscalização e Normalização – DAFN

Pedro Paulo Lemos Machado

Coordenador-Geral de Planejamento, Orçamento e Administração

Liomar Santos Torres

Procurador Federal Chefe

André Pinto Garcia

Planejamento Estratégico 2015 – 2018

Desenvolvido pelo Grupo Técnico designado pela Portaria nº 24, de 17 de Outubro de 2014.

Alessandra Maria Costa e Lima – CODIS/CGPOA
Alexandre Menezes Ribeiro – CGAF/DAFN
José Rodrigues Gonçalves Júnior – CGSI/DINFRA
Maria Izilda Ferreira – CPO/CGPOA
Ruy César Ramos Filho – GABINETE

SUMÁRIO

APRESENTAÇÃO

Trata-se do Planejamento Estratégico do ***Instituto Nacional de Tecnologia da Informação – ITI*** (www.iti.gov.br) para o período de 2015-2018, elaborado por Grupo Técnico de Trabalho – GTT, designado na Portaria n° 24 de 17 de outubro de 2014, publicada no Boletim Interno n° 035, de 17/10/2014.

O planejamento é uma obrigação legal, conforme consta na Constituição Federal de 1988:

> *"Art. 174. Como agente normativo e regulador da atividade econômica, O Estado exercerá, na forma da Lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado."*

A Constituição também estabelece como um dos princípios da Administração Pública a eficiência:

> *"Art. 37. A administração pública direta ou indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência..."*

O Planejamento Estratégico, portanto, é um princípio fundamental da Administração Pública Federal, previsto no Decreto-Lei n° 200/1967:

> *"Art. 6°". As atividades da Administração Federal obedecerão aos seguintes princípios fundamentais:*
>
> *I – Planejamento*
> *II – Coordenação*
> *III – Descentralização*
> *IV – Delegação de Competência e*
> *V – Controle.*
>
> *Art. "7°". "A ação governamental obedecerá a planejamento que vise a promover o desenvolvimento econômico-social do País e a segurança nacional, norteando-se segundo planos e programas elaborados..."*

Assim, em cumprimento ao disposto na Norma e com o intuito de fazer o melhor uso dos recursos disponíveis para atendimento mais qualificado das demandas da sociedade, o Instituto Nacional de Tecnologia da Informação elabora o presente documento que norteará suas ações para o período de 2015 a 2018.

FUNDAMENTOS LEGAIS

O Planejamento Estratégico do ITI foi elaborado a partir de suas competências constitucionais, legais e normativas, previstas nos seguintes documentos (www.iti.gov.br/legislacao):

a) **Medida Provisória nº 2.200-2**, de 24 de Agosto de 2001. - Institui a Infraestrutura de Chaves Pública Brasileira - ICP - Brasil, e dá outras providências.
b) **Decreto nº 3.505**, de 13 de Junho de 2000.- Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
c) **Decreto nº 3.872**, de 18 de Julho de 2001. - Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.
d) **Decreto nº 3.996**, de 31 de Outubro de 2001. - Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
e) **Decreto nº 4.414**, de 07 de Outubro de 2002. - Altera o Decreto no 3.996, de 31 de Outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
f) **Decreto nº 4.689**, de 07 de Maio de 2003. - Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências, e.
g) **Decreto nº 6.605**, de 14 de Outubro de 2008. - Dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP - Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC.

METODOLOGIA

O Planejamento Estratégico 2015-2018 adotou a metodologia denominada *Balanced Scorecard – BSC* com vistas ao alinhamento de objetivos, indicadores, metas e iniciativas institucionais.

O sistema *Balanced Scorecard - BSC*, cuja sigla traduzida significa Indicadores de Desempenho Balanceados, é uma metodologia de medição e gestão de desempenho desenvolvida pelos Professores da Harvard School, Robert Kaplan e David Norton (1992,1997), considerada uma ferramenta de gestão estratégica.

O objetivo fundamental do BSC é traduzir a missão e a estratégia de uma unidade de negócios em objetivos e medidas tangíveis. Em termos mais específicos, o BSC visa viabilizar atividades gerenciais críticas como:

- traduzir a estratégia em objetivos operacionais, por meio de um sistema de mediação;
- estruturar o sistema de medição da organização, evitando a proliferação de indicadores;
- comunicar e associar objetivos e medidas estratégicas;
- planejar, estabelecer metas e alinhar as iniciativas estratégicas, com a estratégia do negócio;
- melhorar a opinião e o aprendizado estratégico;
- fornecer equilíbrio entre o financeiro e outras variáveis relevantes da unidade, entre curto e longo prazos, entre perspectivas internas e externas de desempenho, e entre indicadores de tendências e ocorrências.

Assim, para garantir uma visão integrada da empresa, o BSC propõe descrever a estratégia de forma clara, através de objetivos estratégicos em 4 (quatro) perspectivas: financeira, mercadológica, processos internos e aprendizado & inovação, que resultará no Mapa Estratégico da Unidade.

As quatro perspectivas ajustadas à realidade do ITI que resultarão no seguinte Mapa estratégico:

- ***Orçamento (Financeira)***: destinação prioritária dos recursos orçamentários e financeiros para a realização dos objetivos e ações estratégicas.

- ***Sociedade (Mercadológica)***: direcionamento das ações para atender as necessidades e expectativas dos usuários do serviço de Certificação Digital ICP – Brasil;

- ***Processos Internos***: priorização dos processos de trabalho relevantes e sensíveis, no âmbito de uma estrutura organizacional compatível com a responsabilidade institucional, visando à melhoria constante e ao uso da melhor tecnologia para garantir a segurança de transações e documentos eletrônicos; e

- ***Aprendizado e Inovação***: promoção do desenvolvimento das pessoas, da infraestrutura de recursos, da tecnologia e do conhecimento.

A monitoração do desempenho, focada nesses aspectos críticos integrados, proporciona uma gestão equilibrada do desempenho organizacional.

Por outro lado, foram identificados nós críticos que limitam sobremaneira o cumprimento da missão institucional do ITI, tais como a inexistência de plano de carreira, ausência de quadro

próprio de servidores, quadro de comissões (DAS) incompatível com a atual estrutura da ICP – Brasil, orçamento defasado e incompatível com as necessidades de acompanhamento dos avanços tecnológicos em Segurança da Informação e, por fim, ausência de sede própria.

O impacto dessas limitações pode colocar em risco o Sistema Nacional de Certificação Digital, a gestão do conhecimento e limitar avanços tanto em normalização, pesquisa e tecnologia voltadas à segurança da informação.

Muito embora o Instituto venha há anos buscando sensibilizar os Órgãos envolvidos nessas questões, os avanços são pífios, exigindo, portanto, uma atuação mais estratégica, razão pela qual optou-se em utilizar a metodologia do Planejamento Estratégico Situacional – PES para essas questões mais relevantes.

A opção foi feita depois de analisadas as metodologias de planejamento e gestão disponíveis em âmbito internacional tais como: o método de solução de problemas do sistema de planejamento da qualidade total; o método de planejamento a partir de cenários, com destaque para a prospectiva estratégica de Michel Godet; o Planejamento Estratégico-Situacional; as técnicas de planejamento admitidas pela Gestão Pública por Resultados ou Nova Gestão Pública; o Planejamento Estratégico Corporativo de Michel Porter, o enfoque de gestão estratégica de Michel Crémadez; a concepção e prática do planejamento da escola da organização que aprende; o planejamento na linha do Balanced Scorecard e a lógica de planejamento da análise SWOT.

O Planejamento Estratégico Situacional – PES leva em consideração os efeitos das decisões tomadas hoje sobre o futuro, algumas decorrentes de processos que não controlamos, como é o casos dos nós críticos identificados. Por essa razão, considera importante adotar múltiplos critérios de avaliação e decisão no exercício de simulação e previsão do futuro. O PES propõe trabalhar com o conceito de problemas, oportunidades e ameaças e busca selecionar e identificar problemas reais e distinguir causas de sintomas e consequências, diferentemente dos diagnósticos tradicionais. Como a solução dos nós críticos depende do entendimento, atuação, colaboração de outros atores, o ideal seria o estabelecimento de uma estratégica de ação que contemplasse a interação política baseada na importância de cada ator no processo. (autoridade, persuasão, negociação e conflito).

Finalidade e Competências Institucionais

O ***Instituto Nacional de Tecnologia da Informação- ITI*** foi criado como autarquia federal pelo Art. 12 da Medida Provisória 2.200-2, de 24 de agosto de 2001, com sede e foro no Distrito Federal, vinculada, na forma do Decreto n° 4.566, de 1° de janeiro de 2003, revogado pelo Decreto n° 6.129, de 20 de junho de 2007, à Casa Civil da Presidência da República, com a finalidade de ser a Autoridade Certificadora Raiz - AC Raiz da Infraestrutura de Chaves Públicas Brasileira ICP – Brasil, que tem as seguintes competências:

I - executar as políticas de certificação e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP – Brasil;

II – propor a revisão e a atualização das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP – Brasil;

III – gerenciar os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu, incluindo emissão, expedição, distribuição e revogação desses documentos;

IV – gerenciar a lista de certificados emitidos, revogados e vencidos;

V – executar as atividades de fiscalização e de auditoria das Autoridades Certificadoras – AC, Autoridades de Registro – AR e dos prestadores de serviços habilitados na ICP – Brasil, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP – Brasil;

VI – aplicar sanções e penalidades, na forma da lei; e

VII – emitir certificado para o funcionamento das AC, das AR e dos prestadores de serviço de suporte da ICP – Brasil.

Além das competências operacionais, cumpre ainda ao ITI:

I - promover o relacionamento com instituições congêneres no País e no exterior;

II – celebrar e acompanhar a execução de convênios e acordos internacionais de cooperação, no campo das atividades de infraestrutura de chaves públicas e áreas afins, ouvido o Comitê Gestor da ICP – Brasil;

III – estimular a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infraestrutura de chaves públicas;

IV – estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, autenticidade e integridade de informações eletrônicas; e

V – executar outras atribuições que lhe forem conferidas pelo Comitê Gestor da ICP – Brasil.

Ao ITI compete, ainda, na forma estabelecida pelo Decreto n° 6.605, de 14 de outubro de 2008, atuar como Secretaria Executiva do Comitê Gestor da ICP – Brasil, chefiada pelo Diretor-Presidente do ITI, no papel de Secretário Executivo do Comitê.

O ***Comitê Gestor da Infraestrutura de Chaves Públicas - CG ICP – Brasil,*** instituído pela Medida Provisória n° 2.200-2, de 24 de agosto de 2001, exerce a função de autoridade gestora de políticas da Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil e tem a função de:

I - coordenar o funcionamento da ICP – Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das Autoridades Certificadoras – AC, Autoridades de Registro – AR, Autoridades de Carimbo do Tempo – ACT e demais prestadores de serviço de suporte à ICP – Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV – auditar e fiscalizar a AC Raiz e os seus prestadores de serviço de suporte;

V – estabelecer diretrizes e normas técnicas para a formulação de políticas de certificado e regras operacionais das AC, AR e ACT e definir níveis da cadeia de certificação;

VI – aprovar políticas de certificados e regras operacionais, credenciar e autorizar o funcionamento das AC, das AR, das ACT e demais prestadores de serviço de suporte, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII – identificar e avaliar as políticas de infraestruturas de certificação externas, negociar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP – Brasil, observado o disposto em tratados, acordos ou atos internacionais;

VIII – aprovar as normas para homologação de sistemas e equipamentos de certificação digital no âmbito da ICP – Brasil;

IX – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP – Brasil, de modo a garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança; e

X – aprovar seu regimento interno.

O **Comitê Gestor da ICP – Brasil** é composto por doze membros e respectivos suplentes, sendo cinco representantes da sociedade civil, integrantes de setores interessados e representantes dos seguintes órgãos:

I - Casa Civil da Presidência da República, que coordena o Comitê;

II – Gabinete de Segurança Institucional da Presidência da República;

III – Ministério da Justiça;

IV – Ministério da Fazenda;

V – Ministério do Desenvolvimento, Indústria e Comércio Exterior;

VI – Ministério do Planejamento, Orçamento e Gestão; e

VII – Ministério da Ciência e Tecnologia.

Os representantes da sociedade civil são:

I – Federação Brasileira de Bancos – FEBRABAN;

II – Associação de Juízes Federais do Brasil – AJUFE;

III – Sociedade Brasileira de Computação – SBC;

IV – Confederação Nacional do Comércio de Bens, Serviços e Turismo – CNC.

V – Câmara Brasileira de Comércio Eletrônico - Câmara E-Net.

ORGANOGRAMA FUNCIONAL

O ITI tem a seguinte **estrutura organizacional**:

I – órgão de assistência direta e imediata ao Diretor-Presidente:

a) Gabinete; e

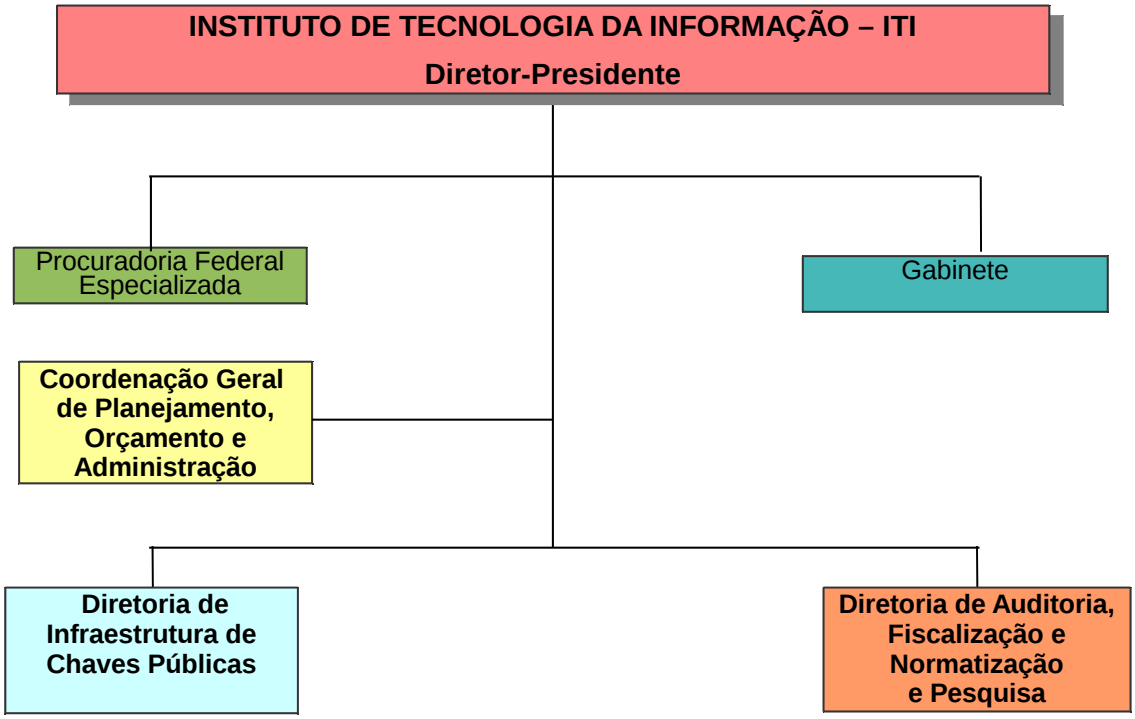
b) Procuradoria Federal Especializada.

II – órgão seccional: Coordenação Geral de Planejamento, Orçamento e Administração;

III – órgãos específicos singulares:

a) Diretoria de Infraestrutura de Chaves Públicas; e

b) Diretoria de Auditoria, Fiscalização e Normalização.



Competências Organizacionais

Gabinete:

I- Assistir ao Diretor-Presidente do ITI em sua representação política social e ocupar-se da comunicação social e do preparo do seu expediente administrativo;

II- Providenciar a publicação e a divulgação das matérias de interesse do ITI;

III- Coordenar o planejamento e a elaboração da pauta de despachos e audiências do Diretor-Presidente;

IV- Providenciar o atendimento às consultas e aos requerimentos formulados pelo Congresso Nacional, encaminhados pela Casa Civil da Presidência da República;

V- Acompanhar a tramitação de projetos de interesse específico do ITI no Congresso Nacional; e

VI- Realizar outras atividades determinadas pelo Diretor-Presidente do ITI.

Procuradoria Federal Especializada:

I- Exercer a representação judicial e extrajudicial do ITI, atuando nos processos em que a Autarquia for autora, ré, oponente ou assistente;

II- Cumprir e velar pelo cumprimento das orientações normativas emanadas da Procuradoria-Geral Federal;

III- Prestar assessoria direta e imediata ao Diretor-Presidente e aos órgãos da Estrutura Regimental do ITI, nos assuntos de natureza jurídica, aplicando-se, no que couber, o disposto no art. 11 da Lei Complementar nº–73, de 10 de fevereiro de 1993;

IV- Examinar e aprovar minutas de editais de licitação, de instrumentos de contratos, de convênios e de outros atos criadores de direitos e obrigações, que devam ser celebrados pelo ITI;

V- Analisar e apresentar soluções sobre questões suscitadas pela aplicação das leis e dos regulamentos relativos às atividades desenvolvidas pelo ITI;

VI- Examinar e emitir pareceres sobre projetos de atos normativos a serem expedidos ou propostos pelo ITI;

VII- Apurar a liquidez e a certeza dos créditos de qualquer natureza, resultantes das atividades implementadas pelo ITI, inscrevendo-os em dívida ativa, para fins de cobrança amigável ou judicial; e

VIII- Realizar outras atividades determinadas pelo Diretor-Presidente do ITI.

Coordenação Geral de Planejamento, Orçamento e Administração:

I- Compete planejar, coordenar e supervisionar a execução das atividades relacionadas aos Sistemas de Pessoal Civil da Administração Federal – SIPEC.

II- Organização e Modernização Administrativa - SOMAD, de Administração dos Recursos de Informação e Informática - SISP, de Serviços Gerais - SISG, de Planejamento e de Orçamento Federal, de Contabilidade Federal e de Administração Financeira, no âmbito do ITI.

Diretoria de Infraestrutura de Chaves Públicas:

I- Dirigir a operação da AC Raiz;

II- Orientar a elaboração de normas e procedimentos operacionais da AC Raiz e da Segurança da Informação para o ITI;

III- Propor a contratação de projetos relativos à operacionalização da AC Raiz, a serem executados com recursos do ITI;

IV- Propor a celebração de convênios, acordos, ajustes e de outros instrumentos congêneres de cooperação técnica, no âmbito de sua atuação;

V- Coordenar e executar a emissão de certificado para as AC de nível imediatamente subsequente ao da AC Raiz da ICP - Brasil; e

VI- Realizar outras atividades determinadas pelo Diretor-Presidente do ITI.

Diretoria de Auditoria, Fiscalização e Normalização:

I- Planejar, coordenar, supervisionar, executar, avaliar e controlar as atividades relacionadas com auditoria, fiscalização e normalização no âmbito da ICP - Brasil e com a definição dos diversos *object identifier - OID*;

II- Atuar como credenciador de empresas de auditoria e auditores independentes para prestação de serviços à ICP - Brasil;

III- Propor a celebração de convênios, acordos, ajustes e de outros instrumentos congêneres de cooperação técnica, no âmbito de sua atuação;

IV- Elaborar propostas de revisão das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP - Brasil; e

V- Realizar outras atividades determinadas pelo Diretor-Presidente do ITI.

MISSÃO E VISÃO

A missão é a razão de ser de uma instituição. Determina o propósito institucional, expressando a sua razão de ser e identificando o alcance de suas ações em termos de serviços e clientes.

A ***Missão*** do Instituto Nacional de Tecnologia da Informação – ITI é:

MISSÃO

"Atuar na inovação, regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente".

VISÃO

"Garantir segurança e validade jurídica às transações e documentos eletrônicos, contribuindo também para o desenvolvimento sustentável."

PRINCÍPIOS E VALORES ORGANIZACIONAIS

Uma Instituição deve contar com ***Princípios*** que balizem o processo decisório e o comportamento da empresa no cumprimento de sua Missão.

O ITI adotou os seguintes ***Princípios:***

• ***Segurança*** – oferecer soluções que possibilitem a segurança, integridade, autenticidade e confidencialidade em transação e documentos eletrônicos;

• **Validade Jurídica** – cumprir e fazer cumprir todas as normas legais e regulamentares que incidem sobre a Certificação Digital ICP – Brasil, de forma que as transações e documentos eletrônicos tenham validade jurídica;

• **Integridade** – garantir que transações e documentos eletrônicos não foram modificados ou destruídos, de maneira não autorizada ou acidental;

• **Autenticidade** – garantir a autoria de transações e documentos eletrônicos;

• **Confidencialidade** – garantir o sigilo de transações e documentos eletrônicos.

O Instituto adotou ainda os seguintes ***Valores***, que explicitam as crenças e convicções que orientam o comportamento das pessoas e que devem ser defendidos pela Instituição, permeando todas as suas atividades e relações.

• ***Credibilidade –*** atuar de forma a garantir a Cadeia de Confiança da ICP – Brasil no âmbito das entidades que compõem a Infraestrutura de Chaves Públicas Brasileira, Governo e Sociedade;

• **Agilidade** – entregar resultados com rapidez e qualidade;

• **Ética** – agir com honestidade e lealdade em todas as ações e relações;

• **Inovação** – buscar soluções inovadoras para garantir a segurança em transações e documentos eletrônicos;

• **Transparência** – praticar atos com legalidade, impessoalidade, moralidade, publicidade e eficiência no desempenho de suas atribuições;

• **Responsabilidade Ambiental** – contribuir para a preservação do meio ambiente ao oferecer soluções que minimizem o uso de recursos naturais e sejam economicamente viáveis, socialmente justos e culturalmente aceitos.

MACROPROCESSOS FINALÍSTICOS E DE APOIO

Macroprocessos Finalísticos

Os macroprocessos finalísticos estão centrados nas seguintes ações: ***"Operacionalização, Manutenção e Modernização da Autoridade Certificadora Raiz – AC RAIZ da ICP – Brasil"*** e ***"Auditoria e Fiscalização nos Prestadores de Serviços de Certificação Digital e Normalização da ICP – Brasil".***

O ITI tem a responsabilidade de assegurar o funcionamento do sistema de certificação nacional "24 horas por dia, sete dias por semana, 365 dias por ano", a uma taxa de 99,99% de disponibilidade, equivalente a uma parada anual de no máximo 52 minutos.

O Instituto tem também a missão de coordenar e executar a emissão, expedição, distribuição, revogação e gerenciamento de certificados para as AC - Autoridades Certificadoras de nível imediatamente subsequente ao da AC Raiz da ICP - Brasil, além de emitir a Lista de Certificados Revogados (LCR).

A modernização da Infraestrutura de Chaves Pública é o grande desafio institucional, pois à Autarquia cabe disponibilizar o *estado da arte* em Certificação Digital, o que exige permanente investimento na segurança do sistema e das mídias utilizadas no processo, que efetivamente garantam a privacidade, autenticidade e integridade das informações eletrônicas realizadas com o uso do Certificado Digital ICP – Brasil.

Avanços Tecnológicos

Ao Instituto cabe propor a celebração de convênios, acordos, ajustes e de outros instrumentos congêneres de cooperação técnica, no âmbito de sua atuação.

Tem ainda a missão de estimular a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infraestrutura de chaves públicas, bem como estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico, voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, autenticidade e integridade de informações eletrônicas.

Para tanto o Instituto mantém Acordos de Cooperação com universidades como é o caso da Universidade Federal de Santa Catarina - USFC, que desenvolve trabalhos de pesquisa e desenvolvimento do criptossistema, além de promover estudos de pós-graduação e doutorado na área de certificação digital, gerando *expertise* na área.

Normalização

O ITI tem a função de orientar a elaboração de normas e procedimentos operacionais da AC Raiz e da sua Segurança da Informação, a serem propostos para o Comitê Gestor da ICP – Brasil, como forma de manter um arcabouço legal e normativo que agregue segurança e padronização ao sistema.

Auditorias e Fiscalizações

A Diretoria de Auditoria, Fiscalização e Normalização tem autonomia para auditar e fiscalizar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP – Brasil para verificar se estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP – Brasil.

Auditorias

Como funcionam

As auditorias no âmbito da Infraestrutura de Chaves Pública Brasileira ICP – Brasil são realizadas de forma independente e reguladas pela Resolução n.º 72, que dita as normas de credenciamento das empresas que realizarão as mesmas. O documento citado também norteia o conceito de metodologia da auditoria, como manuais, roteiros, papéis de trabalho, mapa de riscos, procedimentos, técnicas, formulários, relatórios e modelos.

Os trabalhos de auditoria são regidos pelo Código de Ética e princípios éticos para o exercício das atividades de auditoria interna e independente estabelecidos pelos diversos órgãos reguladores ou de classe, como o Tribunal de Contas da União (TCU), Controladoria Geral da União (CGU), Conselho Federal de Contabilidade (CFC), Comissão de Valores Monetários (CVM), Instituto dos Auditores Independentes do Brasil (Ibracon), *Information Systems Audit and Control Association* (Isaca), Instituto dos Auditores Internos do Brasil (Audibra) e Instituto dos Auditores Internos (IIA).

As auditorias são divididas em dois tipos: pré-operacionais e operacionais. As auditorias pré-operacionais são as realizadas antes do início das atividades do candidato a Prestador de Serviço de Certificação (PSC), quer seja Autoridade Certificadora (AC), Autoridade de Carimbo do Tempo (ACT), Autoridade de Registro (AR) ou Prestador de Serviço de Suporte (PSS).

As operacionais são as realizadas anualmente, considerado o ano civil, em todos os PSC para manutenção do credenciamento junto à ICP – Brasil. Tais auditorias ocorrerão a partir do primeiro ano civil seguinte à data do Diário Oficial da União (DOU) que publicar o credenciamento do PSC.

Credenciamento

O credenciamento de empresas de auditoria na ICP – Brasil exige o cumprimento de requisitos, conforme disposto na Resolução n° 72.

Fiscalizações

A fiscalização tem como objetivo verificar o cumprimento das resoluções, normas, procedimentos e atividades dos Prestadores de Serviço de Certificação (PSC), Autoridades Certificadoras (AC) e Autoridades de Registro (AR), com a finalidade de examinar se as operações de cada um deles, isolada ou conjuntamente, estão em conformidade com as suas respectivas Declarações de Práticas de Certificação (DPC), Políticas de Certificado (PC), Políticas de Segurança (PS) e as demais resoluções e normas gerais estabelecidas para as entidades integrantes da ICP – Brasil.

A fiscalização e o respectivo andamento do processo são normatizados pela Resolução n° 45 – DOC-ICP 09.

O planejamento da fiscalização é semestral e o processo pode variar de 15 a 120 dias, podendo ser iniciado por denúncia feita por usuário de certificação digital da ICP - Brasil ou por constatação de ameaça à confiabilidade da ICP – Brasil. Em caso de denúncia, por determinação do Presidente da AC Raiz ou do Secretário Executivo do Comitê Gestor da ICP - Brasil, a fiscalização poderá atuar sobre qualquer item das normas.

Quando se conclui um processo de fiscalização, pode-se dizer que foi encerrado por conformidade ou por aplicação de penalidade. Dessa forma, as ACs e ARs podem acompanhar o processo de fiscalização.

Responsáveis

As fiscalizações são de responsabilidade do fiscal da ICP - Brasil, servidor vinculado e lotado na Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz e no exercício das funções de fiscal.

Como solicitar

A fiscalização pode ser deflagrada a partir de denúncia feita por usuário de certificação digital da ICP - Brasil ou por constatação de ameaça à confiabilidade da ICP - Brasil, após observação dos relatórios das auditorias.

Homologações

O ITI desenvolveu com o INMETRO – Instituto Nacional de Metrologia, Qualidade e Tecnologia regras que nortearão o Programa de Avaliação de Conformidade (PAC) para equipamentos de certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

A proposta visa migrar de um modelo próprio de reconhecimento e acreditação de hardwares para o sistema INMETRO, internacionalmente reconhecido e que aumentará o número de Laboratórios de Ensaios e Auditorias (LEA) em todo o território nacional.

Em 10 de janeiro de 2013, foi publicada no Diário Oficial da União (DOU) a portaria n° 8 do Instituto Nacional de Metrologia, Qualidade e Tecnologia (INMETRO) que aprovava os Requisitos de Avaliação de Conformidade (RAC) para equipamentos de certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira (ICP - Brasil). Assim, surgia formalmente o processo de certificação no Sistema Brasileiro de Avaliação de Conformidade (SBAC) dos produtos utilizados para a operação da certificação ICP - Brasil (cartões, leitoras, tokens e HSMs).

Na página do ITI - http://www.iti.gov.br/servicos/homologacoes – encontra-se disponibilizada uma breve explicação do funcionamento das homologações, documentos referentes às Resoluções, Instruções Normativas, Manuais de Condutas Técnicas e Adendos, documentos referentes ao processo de homologação e listagem dos laboratórios credenciados.

Também como demanda desta ação, o ITI e o INMETRO iniciaram o processo de revisão dos Manuais de Conduta Técnica (MCT), cujo objetivo é aperfeiçoar a definição de requisitos e ensaios para a adequada migração do processo ao INMETRO.

Macroprocessos de Apoio

Os macroprocessos de apoio essenciais ao funcionamento da Unidade referem-se à execução das atividades relacionadas aos Sistemas de Administração dos Recursos de Informação e Informática (SISP), de Serviços Gerais (SISG) e de Organização e Modernização Administrativa (SOMAD), bem como a gestão do Planejamento, Orçamento (SIOP) e Administração Financeira (SIAFI), levadas a efeito pela Coordenação-Geral Planejamento, Orçamento e Administração - CGPOA.

A CGPOA ainda é responsável pela gestão de todos os contratos de serviços e terceirização de mão de obra que garantem o pleno funcionamento da Autarquia.

Nesse sentido, destacam-se a administração de redes e comunicação levada a efeito pela CGPOA/CODIS, que garante a disponibilidade e segurança da área meio do Instituto, o atendimento a usuários, o apoio no desenvolvimento de projetos básicos na área de tecnologia, quer seja para contratação de serviços e/ou aquisição de equipamentos.

As limitações orçamentárias vêm impactando, sobremaneira, a capacidade produtiva do Instituto, uma vez que o ITI não dispõe de quadro próprio de servidores, valendo-se de mão de obra terceirizada até que seja aprovado seu pleito para adoção do Plano de Carreiras de C&T – Ciência e Tecnologia, para posterior definição do quadro de funcionários, a serem selecionados via concurso público. Por ora, o Instituto se vale de servidores cedidos por outros Órgãos em

cargos de DAS e, no que couber, mão de obra terceirizada.

Infraestrutura de Chaves Públicas Brasileira
ICP - Brasil

Certificação Digital

A Medida Provisória 2.200-2, de 24 de agosto de 2001, deu início à implantação do sistema nacional de certificação digital da Infraestrutura de Chaves Pública Brasileira – ICP – Brasil, criada com o objetivo de regulamentar a utilização da Certificação Digital no País.

O ***Certificado Digital*** funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação feita nos meios virtuais, como a rede de computadores – Internet. Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos assegura a integridade das informações e a autoria das transações.

O Certificado Digital contem dados de seu titular, tais como, número de registro civil, assinatura da Autoridade Certificadora que o emitiu, entre outros atributos, conforme consta na Política de Segurança de cada Autoridade Certificadora.

Portanto, quando se utiliza um certificado digital para gerar um documento eletrônico, inicia-se uma verificação dos dados e da validade do certificado, cujo processo se vale de chaves criptográficas criadas mediante o uso de matemática avançada. A cada entidade (pessoa, empresa, processo ou equipamento) é associada a um par de chaves criptográficas, cuja verificação é realizada pela Autoridade Certificadora que o emitiu de forma automática.

A Certificação Digital é uma ferramenta que confere segurança e validade jurídica a transações realizadas de forma virtual, ou seja, sem presença física do interessado, mas exigem a identificação inequívoca da pessoa que está processando o documento ou transação via Internet.

A certificação digital é uma ferramenta que garante integridade, autenticidade, segurança e validade jurídica aos atos praticados com seu uso, por essa razão é muito utilizada em operações de comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, diversas transações da Receita Federal e de comércio exterior, dentre muitas outras.

O Brasil conta com uma infraestrutura pública, mantida e auditada por um órgão público, no caso o Instituto Nacional de Tecnologia da Informação – ITI, a quem compete executar as políticas de certificação e as normas técnicas e operacionais estabelecidas pelo Comitê Gestor da ICP – Brasil, bem como realizar os processos de credenciamento, fiscalização e auditoria das entidades que compõem a ICP – Brasil, com o objetivo de manter a qualidade dos serviços prestados e o nível de confiança que a sociedade deposita na Infraestrutura.

Avanços da Certificação Digital

O ITI tem como insumo básico tecnologia de ponta, tanto em hardware como em software, para assegurar, desenvolver, manter e prover com disponibilidade mínima de 99.99%, 24 horas por dia, 7 dias por semana, 365 dias por ano, a Infraestrutura de Chaves Públicas Brasileira - ICP – Brasil, de forma a oferecer segurança, autenticidade, integridade, confidencialidade e validade jurídica a transações e documentos eletrônicos, formalizados com o uso de certificados digitais.

A atual estrutura da ICP – Brasil é utilizada cada vez mais em sistemas e aplicações de grande relevância para o desenvolvimento nacional, sendo aplicada nas áreas de Infraestrutura, Desenvolvimento Social Econômica e Produtiva e de Estratégia, Justiça e Defesa, a saber:

Área de Infraestrutura	**Mineral**- PETROBRAS **Comunicação** – Correios **Aeroportuário** – INFRAERO **Energia** – ELETROBRAS e Companhia Paulista de Força e Luz **Transporte –** Conhecimento de Transporte Eletrônico - CT-e
Área de Desenvolvimento Social	**Saúde** – Conselho Federal de Medicina, Conselho Federal de Odontologia, ANVISA, ANS, SIOPS - Transmissão da Declaração de Aplicação de Verbas **Educação** – MEC/PROUNI, FNDE, Carteira Nacional Estudantil, USP – Emissão de Diploma Virtual **Desenvolvimento Social** e Combate à Fome, FOME ZERO/FINEP **Trabalho e Emprego** – Conectividade Social – FGTS/CEF, RAIS - Relação Anual de Informações Sociais, Registro de Entidades Cadastrais, HomologNet- Rescisões contratuais, Processo Judicial Eletrônico no STJ - e-STJ **Previdência Social** – INSS **Cultura Esporte e Turismo** – Lei da COPA, Fundiário – ITR/INCRA **Meio Ambiente** – Licenças Ambientais (CETESB) Conselho nacional de Seguros Privados – CNSP – comercialização de produtos relacionados a planos de saúde e previdência complementar **E-Social** – Sistema de Escrituração Fiscal das Obrigações Fiscais, Previdenciárias e Trabalhistas
Área Econômica e Produtiva	**Desenvolvimento, Indústria e Comércio** – DNRC E INPI, SISCOMEX **Ministério da Agricultura, Pecuária e Abastecimento – MAPA** – Fiscalização de mercadorias de origem animal e vegetal importadas e exportadas. **Econômico Financeiro** – SPB/BACEN, Contrato de Câmbio/BACEN,COMPENSAÇÃO ELETRÔNICA/BACEN-FEBRABAN **Tributação** – NF-e- Nota Fiscal Eletrônica**,** SPED, e-CAC, e-CPF, e-CNPJ, DIRF, DCTF/SRF, SUSEP/FENACOR e Conselho Federal de **Contabilidade** - CFC; COMPRASNET/MPOG
Área de Estratégia, Justiça e Defesa	**Judiciário** – Processo Eletrônico, Peticionamento Eletrônico, Urna Eletrônica (assinatura do software embarcado pelos partidos políticos), BACEN/JUDI, INFOJUS, Conselho Federal da Ordem dos Advogados/OAB, RENAJUD - Sistema de restrições judiciais de Veículos Automotores **Relações Exteriores** – Passaporte Eletrônico (ICAO/PF), Autoridades de Registro em representações Diplomáticas do Brasil no Exterior **Atividades Notariais e de Registro** – ANORGE, IRIB e aplicações estaduais – ABEP, PRODERJ, PODREST/ES, ATI/PE, PROCERGS, IMESP/SP, Sistema Integra permite troca de informações entre cartórios extrajudiciais e órgãos do poder judiciário através da Internet **Defesa** – instalação da futura Autoridade Certificadora do Ministério da Defesa

Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil

O ***Instituto Nacional de Tecnologia da Informação –*** foi criado com o objetivo de operacionalizar, modernizar e fiscalizar a Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil, atuando ainda como a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira – AC Raiz da ICP – Brasil.

A ***Infraestrutura de Chaves Pública Brasileira – ICP – Brasil*** é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para a identificação virtual do cidadão. O modelo adotado pelo Brasil é o de certificação com raiz única, ou seja, com um sistema de certificação centralizado, denominado Autoridade Certificadora Raiz – AC Raiz.

AC Raiz – Autoridade Certificadora Raiz da ICP - Brasil

A ***Autoridade Certificadora Raiz da ICP – Brasil – AC Raiz*** desempenha um papel crucial no Sistema Nacional de Certificação Digital. A AC Raiz é a primeira autoridade da cadeia de certificação, portanto todas as transações efetuadas com um Certificado Digital da ICP – Brasil necessariamente são submetidas ao Sistema Nacional de Certificação Digital em tempo real, que validará ou não a transação. Para tanto, compete ao ITI assegurar o funcionamento do sistema 24 horas por dia, 7 dias por semana, 365 dias por ano, a uma taxa de disponibilidade 99,99%.

A AC Raiz é responsável pela emissão, expedição, distribuição, revogação e gerenciamento dos certificados das Autoridades Certificadoras credenciadas, chamadas de Autoridades Certificadoras de 1° Nível.

A AC Raiz também está encarregada de emitir e publicar a sua lista de Certificados Revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviços credenciados na ICP – Brasil.

AC - Autoridade Certificadora

Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP - Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais. Tem a responsabilidade de verificar se o titular do certificado possui a chave privada que corresponde à chave pública que faz parte do certificado. Cria e assina digitalmente o certificado do titular, onde o certificado emitido pela AC representa a declaração da identidade do titular, que possui um par único de chaves (pública/privada).

Cabe também à AC emitir listas de certificados revogados (LCR) e manter registros de suas operações sempre obedecendo às práticas definidas na Declaração de Práticas de Certificação (DPC). Além de estabelecer e fazer cumprir, pelas Autoridades Registradoras (ARs) a ela vinculadas, as políticas de segurança necessárias para garantir a autenticidade da identificação realizada.

AR - Autoridade de Registro

Uma Autoridade de Registro (AR) é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

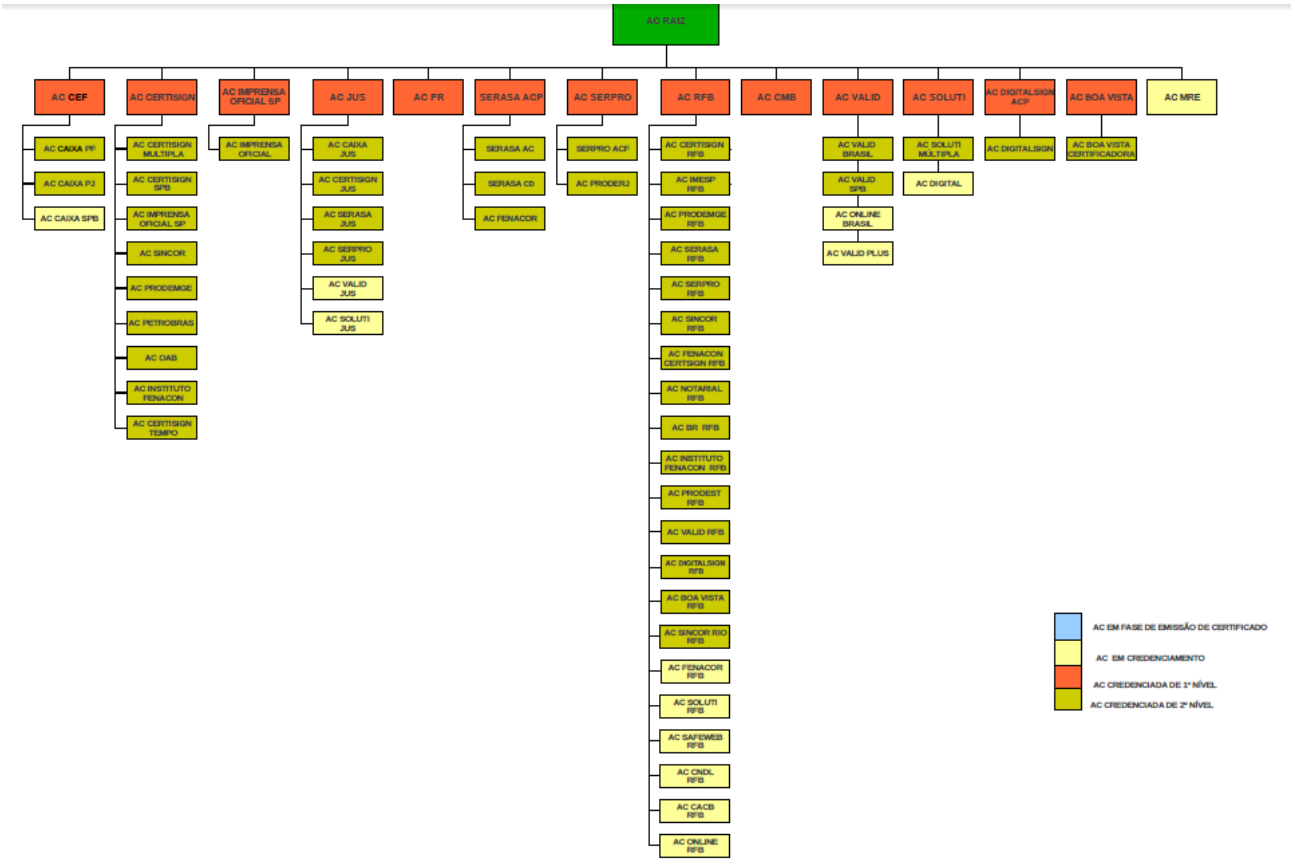
ACT - Autoridade Certificadora do Tempo

Uma Autoridade Certificadora do Tempo (ACT) é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir Carimbos do Tempo. A ACT tem a responsabilidade geral pelo fornecimento do Carimbo do Tempo, conjunto de atributos fornecidos pela parte confiável do tempo que, associado a uma assinatura digital, confere provar a sua existência em determinado período.

Na prática, um documento é produzido e, em seguida, ele recebe os atributos ano, mês, dia, hora, minuto e segundo, atestado na forma da assinatura realizada com certificado digital servindo assim para comprovar sua autenticidade.

Estrutura da ICP - Brasil

A Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil está composta das seguintes Autoridades Certificadoras de 1º Nível e de 2º Nível.



SERPRO - Serviço Federal de Processamento de Dados

Primeira Autoridade Certificadora de 1º nível credenciada pela ICP - Brasil, a empresa busca, desde a criação de seu Centro de Certificação Digital - CCD, em 1999, divulgar o uso dessa tecnologia para os vários segmentos com que trabalha.

CAIXA ECONÔMICA FEDERAL

Única instituição financeira credenciada como Autoridade Certificadora ICP - Brasil, a Caixa Econômica Federal tem trabalhado também para que a certificação digital integre serviços que resultem em melhoras para seus funcionários, clientes e titulares das contas de Fundo de Garantia por Tempo de Serviço – FGTS.

SERASA EXPERIAN

Autoridade Certificadora do setor privado, a Serasa fornece a segurança dos certificados digitais para quase todos os grupos financeiros participantes do Sistema de Pagamentos Brasileiro (SPB).

RECEITA FEDERAL DO BRASIL

A Receita Federal do Brasil (RFB) disponibiliza uma grande quantidade de serviços com o objetivo de simplificar ao máximo a vida dos contribuintes, facilitando o cumprimento espontâneo das obrigações tributárias para os que possuem certificados digitais ICP – Brasil.

CERTISIGN

A Certisign tem duplo foco no ramo da certificação digital. Além de fornecer a ferramenta tecnológica, o grupo desenvolve soluções para uso exclusivo com certificados digitais ICP – Brasil.

IMPRENSA OFICIAL DO ESTADO DE SÃO PAULO

A Imprensa Oficial é a Autoridade Certificadora Oficial do Estado de São Paulo credenciada para oferecer produtos e serviços de certificação digital para os poderes executivo, legislativo e judiciário, incluindo todas as esferas da administração pública, direta e indireta, nos âmbitos federal, estadual e municipal.

AC JUS

A AC-JUS alavancou definitivamente a implantação da Certificação Digital no Judiciário com o desenvolvimento de aplicações para comunicação e troca de documentos, agora com validade legal, viabilizando dessa forma o advento do Processo Judicial Eletrônico (PJ-e).

AC PR

Credenciada a emitir Certificados Digitais totalmente aderentes às normas, padrões estabelecidos pelo Comitê Gestor da ICP-Brasil, a Autoridade Certificadora da Presidência da República - ACPR foi criada em abril de 2002, por uma iniciativa da Casa Civil, no âmbito do governo eletrônico (e-Gov). A ACPR emite certificados para autoridades e servidores da Presidência da República e da Vice-Presidência da República e para autoridades e servidores do Poder Executivo Federal que necessitam utilizar certificado digital para autenticação em aplicativos geridos pela PR.

CASA DA MOEDA DO BRASIL

Entre as mais antigas instituições públicas brasileiras, a instituição consolida o objetivo de modernização de sua estrutura produtiva e administrativa, bem como se habilita para atender ao mercado de segurança na era virtual.

VALID CERTIFICADORA DIGITAL

A AC Valid, 10ª entidade a credenciar-se como AC de 1° nível, atua no mercado de certificação digital focando suas atividades em tecnologias que resultem na prestação de serviços. Além da emissão dos certificados, a Valid oferece serviços de tecnologia para infraestrutura de chaves públicas, consultoria e suporte no comando de processos e atividades de apoio a Autoridades de Registro.

SOLUTI CERTIFICAÇÃO DIGITAL

Especializada em tecnologia da informação com atuação em todo o território brasileiro, em 2012 a Soluti tornou-se a 11ª Autoridade Certificadora (AC) de 1° nível vinculada à ICP – Brasil. A Soluti já atuava como Autoridade de Registro (AR) em vários estados do País oferecendo serviços, produtos e soluções em certificação digital.

AC DIGITALSIGN

A Digitalsign é uma empresa portuguesa, que através da Digitalsign Certificadora – empresa brasileira, tornou-se a 12ª Autoridade Certificadora - AC de 1º nível da ICP – Brasil. Grupo é composto pelas empresas DigitalSign Portugal, AET Europe e Thomas Greg & Sons.

AC BOA VISTA

A AC Boa Vista é a unidade de negócios de Certificação Digital da Boa Vista Serviços e completa a oferta da empresa com soluções para a tomada de decisões sustentáveis de crédito e gestão de negócios. Controlada por brasileiros, a Boa Vista opera o cadastro positivo no país e investe continuamente em tecnologia de ponta para atender à sua carteira de clientes em todo o território nacional.

Objetivos Estratégicos do ITI

O grande objetivo estratégico do Instituto tem sido a ***Massificação do Uso da Certificação Digital - ICP – Brasil.***

No âmbito do PPA 2012-2015, muito embora não tenha sob sua responsabilidade um programa temático específico, sua contribuição ao Governo, à Sociedade e ao Cidadão está inserida no contexto do ***Programa 2038 – Democracia e Aperfeiçoamento de Gestão Pública***, amparada no ***Objetivo*** de "Ampliar a Oferta de Serviços Públicos de Excelência", conforme abaixo:

Programa Democracia e Aperfeiçoamento da Gestão Pública (Código 2038)

Objetivo: Ampliar a oferta de serviços públicos de excelência ao cidadão, às empresas e às demais organizações da sociedade, mediante a melhoria dos marcos legais, dos processos de trabalho e da tecnologia da informação.

Iniciativa: Massificação e Aperfeiçoamento da Certificação Digital ICP – Brasil e outras tecnologias de segurança da informação e identificação digital, necessárias às transações eletrônicas de interesse da União, dos Estados, dos Municípios e da Sociedade, mediante a garantia de pleno funcionamento da Infraestrutura de Chaves Públicas Brasileira e de Carimbo do Tempo da ICP – Brasil, como forma de assegurar sua interoperabilidade, capilaridade, acessibilidade, e eficácia jurídica às transações e documentos eletrônicos, bem como contribuir para a preservação do meio ambiente ao permitir a desmaterialização de processos e documentos.

No âmbito Orçamentário, o Instituto conta com as seguintes ações finalísticas:

4858 – *Promoção e Disseminação do Uso da Certificação Digital ICP - Brasil*
4912 – *Auditoria e Fiscalização nos Prestadores de Serviços de Certificação Digital e Normalização da ICP – Brasil*
4917 – *Operacionalização, Manutenção e Modernização da Autoridade Certificadora Raiz da Infraestrutura da ICP - Brasil*

As ações orçamentárias para gestão da Unidade estão inseridas na programática - 2101 – Programa de Gestão e Manutenção da Presidência da República – Ações 2000 – Administração da Unidade.

Sob o ponto de vista das despesas obrigatórias, o Instituto dispõe das seguintes ações:

09HB – Contribuição da União, de suas Autarquias e Fundações para o Custeio do Regime de Previdência dos Servidores Públicos Federais
2004 – Assistência Médica e Odontológica aos Servidores, Empregados e seus Dependentes
2010 – Assistência Pré-Escolar aos Dependentes dos Servidores e Empregados
2011 – Auxílio-Transporte aos Servidores e Empregados
2012 – Auxílio-Alimentação aos Servidores e Empregados
20CW – Assistência Médica aos Servidores e Empregados – Exames Periódicos
00H1 – Pagamento de Pessoal Ativo da União.

ANÁLISE AMBIENTAL – MATRIZ SWOT (part. I)

Para a definição das Diretrizes Estratégicas é necessário analisar os cenários externos (ameaças e oportunidades) e internos (pontos fortes e fracos) no âmbito da matriz SWOT – ***S****trengths,* ***W****eaknesses,* ***O****pportunities and* ***T****hreats*. A análise ambiental é referencial obrigatório na formulação do Plano de Gestão, de modo a considerar os fatores intervenientes que impactam positiva e negativamente o funcionamento da organização, o cumprimento de sua missão institucional, conformidade da visão de futuro e o alcance dos resultados pretendidos.

*Nes*sa perspectiva cumpre ressaltar que as ações do ITI estão previstas no PPA 2012-2015 – Plano Plurianual – o Plano Mais Brasil, estruturado a partir da dimensão estratégica que deu origem a Programas nos quais estão contidos os desafios e os compromissos de governo para o futuro imediato: os próximos quatro anos.

As ações do ITI estão inseridas no contexto do Programa 2038 – Programa Democracia e Aperfeiçoamento da Gestão Pública, cujo objetivo é:

> "Ampliar a oferta de serviços públicos de excelência ao cidadão, às empresas e às demais organizações da sociedade, mediante a melhoria dos marcos legais, dos processos de trabalho e da tecnologia da informação".

As responsabilidades institucionais do ITI no âmbito estratégico governamental estão consubstanciadas na iniciativa:

> **"*Massificação e aperfeiçoamento da Certificação Digital ICP – Brasil e outras tecnologias de segurança da informação e identificação digital necessárias às transações eletrônicas de interesse da União, dos Estados, dos Municípios e da Sociedade, mediante a garantia de pleno funcionamento da Infraestrutura de Chaves Públicas Brasileira e de Carimbo do Tempo da ICP – Brasil, como forma de assegurar sua interoperabilidade, capilaridade, acessibilidade e eficácia jurídica às transações e documentos eletrônicos, bem como contribuir para a preservação do meio ambiente ao permitir a desmaterialização de processos e documentos".***

Nesse âmbito, atualmente conta com três ações orçamentárias finalísticas:

4858 – Promoção e Disseminação do Uso da Certificação Digital – ICP - Brasil
4912 – Auditoria e Fiscalização nos Prestadores de Serviço de Certificação Digital e Normalização da ICP – Brasil
4917 – Operacionalização, Manutenção e Modernização da Autoridade Certificadora Raiz da Infraestrutura da ICP – Brasil

A dinâmica do ambiente em que se insere o ITI traduz-se em ameaças, que são as situações que podem colocá-lo em risco, e oportunidades, que podem ser aproveitadas para impulsionar o seu desenvolvimento.

São consideradas ***ameaças*** ao desenvolvimento das atividades do ITI:

Estrutura operacional e orçamentária defasada, haja vista que o Instituto ainda opera com a mesma estrutura organizacional desde sua criação em 2002 e não dispõe de quadro de carreira e quadro de funcionários próprio, obrigando-o a valer-se de serviços terceirizados, que muitas vezes têm alcance limitado e forte impacto nas despesas discricionárias de seu orçamento;

- Permanente avanço tecnológico em segurança da informação, o que exige cada vez mais investimentos em pesquisa e desenvolvimento de novas tecnologias voltadas a garantir interoperabilidade e a segurança em transações e documentos eletrônicos;
- Avanço do uso da Certificação Digital em processos críticos para a sociedade brasileira, que impõem alta disponibilidade de serviços e permanente monitoramento de ataques de hackers, fraudes, e outras tentativas de invasão do sistema;
- Significativo crescimento da Infraestrutura de Autoridades certificadoras e Prestadores de Serviços, o que exige cada vez mais recursos humanos, físicos e lógicos capazes de auditar e fiscalizar essa rede, como forma de garantir sua conformidade a padrões e procedimentos estabelecidas pela ICP – Brasil;

Por outro lado, o ambiente externo apresenta ***oportunidades***, tais como:

- A Certificação Digital oferece ganhos em termos de economicidade, agilidade, segurança, validade jurídica em transações e documentos eletrônicos, cada vez mais visíveis, reconhecidas e valorizadas pela sociedade brasileira;
- Alta disponibilidade da ferramenta 24horas por dia, 7dias por ano, a uma taxa de 99,99%, o que garante seu uso e forma ininterrupta, a qualquer tempo e independente de sua localização;
- Crescente oferta de novas aplicações que se utilizam da Certificação Digital como ferramenta de segurança e validade jurídica tanto no âmbito governamental como privado;
- Ampla gama de aplicações públicas e privadas com potencial para uso da ferramenta;
- Publicação da Lei 12.682/2012, que concede ao documento digitalizado o mesmo valor legal do documento em papel, desde que utilizado o Certificado Digital padrão ICP – Brasil, como ferramenta exclusiva de segurança, confiabilidade e validação das digitalizações. A Lei promoverá avanços importantes no uso de documentos eletrônicos e na utilização da certificação digital ICP – Brasil;
- Amplo desenvolvimento do *e-commerce* alicerçado no uso de certificado digital ICP – Brasil;
- Incentivo à desmaterialização de processos, no âmbito do Processo Eletrônico (PEN);
- O uso da Certificação Digital tem se revelado uma alternativa para a redução do custo Brasil e efetiva contribuição para a sustentabilidade (“*Green Economy*”), ao viabilizar ações que reduzem o consumo de papel, tinta, madeira e água; e
- Desconhecimento da sociedade quanto aos benefícios da ferramenta.

Com relação ao ambiente interno, os ***pontos fracos*** que podem limitar a atuação e o desenvolvimento organizacional, tem a ver com as seguintes variáveis:

1. Estrutura organizacional e orçamentária defasada, haja vista que o Instituto ainda opera com a mesma estrutura organizacional desde sua criação em 2002 e não dispõe de quadro de carreira e quadro de funcionários próprio, obrigando-o a valer-se de serviços terceirizados, que muitas vezes têm alcance limitado e forte impacto nas despesas discricionários de seu orçamento. Áreas críticas, como a de controle da infraestrutura de comunicações, redes, sistemas e segurança da informação da área meio sofrem com ausência de profissionais próprios e suficientes para a sua gestão. Na área finalística, essa limitação vai além, retardando avanços na área de pesquisa e desenvolvimento, uma vez que os recursos são alocados prioritariamente na operacionalização da Infraestrutura de Chaves Públicas, haja vista sua alta disponibilidade (24horas por dia, 7 dias por semana – 99.99%);
2. Carência de profissionais especializados na área de pesquisa em C&T e Desenvolvimento Tecnológico, o que obriga o Instituto a valer-se de Acordos de Cooperação e Termos de Descentralização de Créditos para garantir a compatibilidade do sistema com avanços de novas Tecnologias da Informação;
3. Ausência de sede própria para integração do ambiente seguro. Atualmente o

Órgão ocupa um prédio monousuário alugado, sendo obrigado a manter a sala cofre nas dependências da Presidência da República, o que torna sua administração mais cara e complexa;
4. Alta demanda de monitoramento do sistema com relação a tentativas de invasão e fraudes, permanente investimento em interoperabilidade e crescente demanda por homologação de artefatos;
5. Alta demanda para pesquisa e alinhamento de padrões e normas internacionais, com vista à interoperabilidade.

Em contrapartida, o ambiente interno apresenta como ***pontos fortes***:

- Benefícios da Certificação Digital ICP-Brasil: segurança, economicidade, eficiência no uso de recursos, redução de custos, agilidade, integridade, autenticidade, privacidade e validade jurídica em transações e documentos eletrônicos;
- Participação acadêmica em pesquisa científica e desenvolvimento tecnológico;
- Comprometimento e dedicação do quadro de DAS; composto por profissionais altamente capacitados com formação e experiência em TIC;
- Fomento e apoio tecnológico para o desenvolvimento de novas aplicações;
- Investimento no desenvolvimento de tecnologia nacional na área de segurança da informação;
- Reconhecimento internacional, em especial na América Latina, como órgão de referência em segurança da informação.

A análise ambiental evidenciou a necessidade de atuação em determinadas frentes, cujo êxito é considerado fundamental para o cumprimento da missão e o alcance da visão. Dessa forma, foram traçadas as ***Diretrizes Estratégicas*** que sinalizam a necessidade de atuação nas seguintes frentes:

1. ***Operacionalização, Manutenção e Modernização do Sistema Nacional de Certificação Digital ICP – Brasil***
2. ***Auditoria e Fiscalização do Sistema Nacional de Certificação Digital da ICP - Brasil***
3. ***Normalização e Pesquisa em Criptografia e Segurança da Informação***
4. ***Prospecção e Evolução Tecnológica em Criptografia e Segurança da Informação***
5. ***Fomento a aplicações com uso da Certificação Digital ICP - Brasil***
6. ***Promoção e Disseminação do Uso da Certificação Digital – ICP – Brasil: Sensibilização e Capacitação***
7. ***Macroprocessos de Apoio e Reestruturação Organizacional***
8. ***Reestruturação Orçamentária***
9. ***Monitoramento de Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP Brasil.***

Definidas as Diretrizes Estratégicas, as áreas foram instadas a desenvolver as ações que permitirão o cumprimento dos objetivos estratégicos traçados.

Diretrizes e Objetivos Estratégicos

1. Operacionalização, Manutenção e Modernização do Sistema Nacional de Certificação Digital ICP – Brasil.

Objetivo 1.1:	Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil
Ação:	Aperfeiçoamento e expansão das Autoridades Credenciadas para emissão de certificados digitais e manutenção da estrutura física para operação da AC Raiz da ICP – Brasil e da Entidade de Carimbo de Tempo
Meta:	Manutenção de dois Centros de Certificação Digital (principal e contingência)
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável	CGO – André Machado Caricatti

Objetivo 1.2:	Manter ambiente seguro principal para a AC Raiz
Ação:	Manter a estrutura física para operação da AC Raiz da ICP – Brasil e Entidade de Auditoria de Tempo
Meta	Contratação de empresa especializada para a manutenção preventiva e corretiva dos subsistemas do ambiente seguro. Contratação dos meios físicos e lógicos para acesso à Internet. Contratação dos meios físicos e lógicos de contingência para o acesso à Internet. Garantir a disponibilidade de 99,99%, conforme legislação vigente.
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Objetivo 1.3:	Manter ambiente seguro de contingência para a AC Raiz
Ação:	Manter estrutura física de contingência para operação da AC Raiz da ICP – Brasil e Entidade de Carimbo de Tempo
Meta:	Prover estrutura física de contingência para operação da AC Raiz da ICP – Brasil e Entidade de Auditoria de Tempo. Contratação de hospedagem do ambiente de contingência para a Autoridade Certificadora Raiz e da Entidade de Auditoria de Tempo da ICP – Brasil. Contratação dos meios físicos e lógicos para o acesso à Internet do ambiente de contingência. Contratação dos meios físicos e lógicos de contingência para o acesso à Internet do ambiente de contingência. Garantir a disponibilidade de 99,99%, conforme legislação vigente.
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Objetivo 1.4:	Modernizar os subsistemas do ambiente seguro do ITI
Ação:	Manter os subsistemas do ambiente seguro da AC Raiz atualizados.
Meta	Adequar os subsistemas, mantendo a garantia e suporte continuados dos fabricantes e/ou empresa especializada: -Adequação e atualização tecnológica do subsistema de climatização -Adequação e atualização tecnológica do subsistema de detecção e combate à incêndio -Adequação e atualização tecnológica do subsistema de supervisão e controle -Adequação das instalações técnicas da DINFRA e instalação de solução de operação e monitoramento remoto (NOC)
Prazo:	2015, 2016, 2017
Recursos Orçamentários	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Objetivo 1.5:	Prover Infraestrutura para operação da Entidade de Carimbo do Tempo
Ação:	Manter hardware e software para operação da Entidade de Carimbo de Tempo
Meta:	Garantir a disponibilidade de 99,5%, conforme legislação vigente. Contratação de suporte, manutenção preventiva e corretiva para os sistemas e equipamentos Bry. Contratação de suporte, manutenção preventiva e corretiva para os sistemas e equipamentos Thales. Aquisição de infraestrutura de contingência para a Entidade de Carimbo de Tempo. Aquisição de infraestrutura de homologação para a Entidade de Carimbo de Tempo.
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGO – André Machado Caricatti

Objetivo 1.6:	Contratar auditoria independente
Ação:	Manter certificação de operação da AC Raiz, em conformidade com os normativos vigentes.
Meta:	Manter certificação periódica emitida por terceira parte de operação da AC Raiz de acordo com os normativos.
Prazo:	2015, 2016, 2017, 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Objetivo 1.7:	Aperfeiçoar o processo de identificação do sistema ICP - Brasil
Ação:	Mitigar os riscos decorrentes das fragilidades no processo de identificação do Sistema Nacional de Certificação Digital ICP - Brasil.
Meta:	Propor e implementar melhorias no sistema de identificação para mitigar os riscos decorrentes das fragilidades identificadas.
Prazo:	2015, 2016, 2017
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	Gabinete – Eduardo Magalhães de Lacerda Filho

Objetivo 1.8:	Fomentar o sistema de Homologação da ICP-Brasil
Ação:	Manter um sistema de homologação de hardware para a ICP - Brasil propiciando a migração para o sistema SBAC
Meta	Propiciar a migração do sistema de homologação ICP-Brasil para o INMETRO (SBAC) propiciando o reconhecimento internacional das certificações emitidas.
Prazo:	2015, 2016
Recursos Orçamentários	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGO – André Machado Caricatti

2. Auditoria e Fiscalização do Sistema Nacional de Certificação Digital da ICP - Brasil

Objetivo 2.1:	4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Ação:	Certificar, por meio de auditorias e fiscalizações operacionais e de credenciamento, a conformidade dos processos, procedimentos operacionais e atividades dos prestadores de serviço de certificação, com as suas respectivas declarações de prática de certificação, suas políticas de certificação, a política de segurança e demais documentos, regulamentações e normas gerais estabelecidos para as entidades em credenciamento ou integrantes da ICP – Brasil, por meio de processo de auditoria e fiscalização consubstanciados em relatórios, devendo as irregularidades serem acompanhadas até sua correção.
Meta	100 relatórios de auditoria e fiscalização/ano
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Responsável:	CGAF – Pedro Pinheiro Cardoso

3. Normalização e Pesquisa em Criptografia e Segurança da Informação

Objetivo 3.1:	Normalização e Pesquisa
Ação:	Realizar pesquisas e propor a revisão, atualização e suplementação das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP – Brasil, observados os demais aspectos jurídicos sobre a matéria, com vistas a garantir a adoção de padrões de interoperabilidade e segurança compatíveis com as normas brasileiras e internacionais.
Meta	- revisão normativa da ICP-Brasil a fim de adequar-se aos regulamentos e normas internacionais (quando aplicáveis) sobre o certificação digital e assuntos correlatos - consolidação do padrão de assinatura PADES (2015) - consolidação do conjunto normativa dos MCT para atender ao novo processo de homologação via SBAC/INMETRO (2016) -Definições dos diversos OID -Emissão e gerenciamento de PAs e LPA
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Responsável:	CGNP – Wilson Roberto Hirata

4. Prospecção e Evolução Tecnológica em Criptografia e Segurança da Informação

Objetivo 4.1:	Modernizar a infraestrutura tecnológica da AC Raiz da ICP – Brasil
Ação:	Prover infraestrutura de rede, armazenamento e segurança da AC Raiz com sistemas e equipamentos atualizados tecnologicamente.
Meta:	Substituir e atualizar os equipamentos de armazenamento da rede SAN em final do ciclo de vida para o ambiente principal e de contingência Aquisição de equipamentos para complementação e ampliação da infraestrutura de segurança da AC Raiz. Aquisição de equipamentos para complementação e ampliação da capacidade de balanceamento de enlaces e cargas para a infraestrutura de rede da AC Raiz. Atualização do parque tecnológico para o ambiente seguro principal e de contingência Aquisição de ferramentas para análise de mídias e sistemas. Aquisição de software de virtualização para o ambiente seguro principal/contingência.
Prazo:	2015 e 2016
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Objetivo 4.2:	Desenvolver e manter criptossistema em código aberto com tecnologia nacional
Ação:	Manter o hardware e software (SGC-Ywapa, Ywyra e Hawa) da AC-Raiz da ICP Brasil atualizados, de acordo com os requisitos operacionais e de algoritmos criptográficos.
Meta:	Produto: sistema implantado/Unidade de Medida: % de execução física/Quantidade anual: 1 Atender as demandas da ICP Brasil, conforme prazos estabelecidos. Manutenção do sistema de emissão de certificados digitais da Autoridade Certificadora Raiz (*Ywapa*). Manutenção do sistema de emissão de certificados de Autoridades Certificadoras intermediárias (*Ywyra*). Manutenção do sistema de emissão de certificados digitais para o usuário final (*Hawa*). Manutenção do hardware seguro da ICP Brasil. Manutenção do software do hardware seguro da ICP Brasil.
Prazo:	2015, 2016, 2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 7264 – Desenvolver criptossistema em código aberto com tecnologia nacional
Responsável:	DINFRA – Ruy César Ramos Filho

5. Fomento a aplicações com uso da Certificação Digital ICP - Brasil

Objetivo 5.1:	Fomento da utilização de certificado digital na soluções de TI utilizadas no âmbito do ITI
Ação:	Incentivar a utilização de certificação digital nos serviços prestados pela CGPOA/CODIS aos colaboradores do ITI para alinhar as soluções de TI aos mecanismos de segurança definidos pelo próprio Instituto.
Meta	**Fornecimento de soluções relacionadas com certificação digital** Indicador: quantidade de soluções de TI suportadas pela CGPOA/CODIS que utilizam tecnologia de certificação digital. Métrica: ao menos duas soluções suportadas pela CODIS a cada dois anos **Fornecimento de certificado digital aos colaboradores do Instituto.** Indicador: % de colaboradores que possuem certificado digital válido. Meta: 95% dos colaboradores devem possuir certificado digital válido.
Prazo:	2015, 2016, 2017 e 2018
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	CGPOA/CODIS – Alessandra Lima

Objetivo 5.2:	Fomentar o desenvolvimento de novas aplicações que façam uso da Certificação Digital ICP Brasil no âmbito governamental e privado.
Ação:	Incentivar e prestar apoio técnico ao desenvolvimento de novas aplicações que façam uso da Certificação Digital ICP Brasil e os produtos associados no âmbito governamental e privado.
Meta	Manutenção do Assinador Digital de Referência (ADRB) padrão ICP-Brasil Manutenção do Sistema de Gerenciamento de Certificados de Atributos (SGCA) Desenvolvimento do *middleware* padrão ICP-Brasil Manutenção do verificador de conformidade do padrão de assinatura da ICP-Brasil Participar em fóruns, câmaras técnicas, comitês a fim de representar o ITI nos debates relacionados à certificação digital.
Prazo:	2015, 2016, 2017 e 2018
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo

6. Promoção e Disseminação do Uso da Certificação Digital – ICP – Brasil: Sensibilização e Capacitação

Objetivo 6.1:	Apresentar a sociedade cases que demandam a tecnologia ICP – Brasil, sensibilizar gestores públicos e privados em relação ao tema e estimular a adoção de tecnologias mais sustentáveis e a eliminação do uso de insumos.
Ação:	Realizar o Fórum de Certificação Digital - CertForum
Meta	Realizar duas etapas do evento anualmente, sendo uma em Brasília - DF
Prazo:	2015 2016,2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	ASCOM – Edmar da Silva Araújo

Objetivo: 6.2:	Produzir material jornalístico, publicitário e de marketing que garanta a disseminação e o conhecimento da tecnologia ICP – Brasil e registre para a memória do ITI, eventos relevantes.
Ação:	Produção de boletim semanal, boletim interno, revista institucional, vídeo institucional notas e release á imprensa e atualização das mídias sociais com os devidos conteúdos produzidos pela ASCOM.
Meta	Manter os vários segmentos da sociedade informados sobre perspectivas mais aprofundadas dos temas sobre os benefícios e aplicações da Certificação Digital ICP–Brasil.
Prazo:	2015,2016,2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	ASCOM – Edmar da Silva Araújo

7. Macroprocessos de Apoio e Reestruturação Organizacional

Objetivo 7.1 :	Viabilizar a Implementação e Execução da Coleta Seletiva de Resíduos Recicláveis
Ação:	Tomar as providências necessárias à implementação da Coletiva Seletiva de Resíduos Recicláveis, de acordo com o Decreto n° 5.940, de 05/10/2066.
Meta:	Implantar a infraestrutura necessária e iniciar à Coletiva Seletiva de Resíduos Recicláveis – Unidade: 5 (percentual) de implantação.
Prazo:	2015 – 100%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues

Objetivo 7.2:	Gestão do Almoxarifado
Ação:	Desenvolver ações para o aperfeiçoamento da gestão do almoxarifado, de forma que seja possível manter e controlar o estoque físico e os correspondentes registros digitais, evitando-se também a aquisição de material via suprimento de fundos e dispensa de licitação.
Meta:	Manter e controlar o estoque do almoxarifado de acordo com as necessidades do Órgão – Unidade: inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação.
Prazo:	2015–Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação 2016–Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação 2017–Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação 2018-Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues

Objetivo 7.3 :	Controle Patrimonial
Ação:	Aperfeiçoar o controle do acervo patrimonial do Instituto, de acordo com a legislação vigente, além de executar política de desfazimento regular de bens inservíveis, de modo a evitar a onerosidade com estoque e depósito dessa natureza de material.
Meta:	Eliminar as inconsistências e manter o sistema atualizado – Unidade: Zerar inconsistências e não manter estoque de bens inservíveis
Prazo:	2015 – Não apresentar inconsistências e não manter estoque de bens inservíveis 2016 – Não apresentar inconsistências e não manter estoque de bens inservíveis 2017 – Não apresentar inconsistências e não manter estoque de bens inservíveis 2018 – Não apresentar inconsistências e não manter estoque de bens inservíveis
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues

Objetivo 7.4:	Capacitação de Servidores Públicos Federais em Processo de Qualificação e Requalificação
Ação:	Promover a qualificação e requalificação de pessoal com vistas à melhoria continuada dos processos de trabalho, dos índices de satisfação pelos serviços prestados à sociedade e do crescimento profissional.
Meta:	Elaborar levantamento anual das necessidades de treinamento e participação em eventos e seminários, de forma otimizar a forma de contratação, evitando-se a dispensa de licitação. Unidade: Autorizar o treinamento ou participação em eventos e seminários, congressos e afins de, pelo menos, 20% do quadro de pessoal, passível de ser contemplado.
Prazo:	2015 – 20% 2016 – 20% 2017 – 20% 2018 – 20%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CGP – Roberto Bueno de Assunção

Objetivo 7.5:	Exame Periódico de Pessoal sem Vínculo
Ação:	Desenvolver ações necessárias à execução dos exames de saúde periódicos, em especial, para o pessoal sem vínculo empregatício.
Meta:	Viabilizar a realização de exames de saúde periódicos, em especial, para o pessoal sem vínculo empregatício. Unidade: fazer com que 100% do pessoal sem vínculo empregatício realize os exames de saúde periódico.
	2015 – 100% 2016 – 100% 2017 – 100% 2018 – 100%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CGP – Roberto Bueno de Assunção

Objetivo 7.6 :	Melhoria do Processo de Conformidade Contábil
Ação:	Identificação dos processos que necessitam de aprimoramento das ações, para que a conformidade seja realizada, de acordo com padrões de qualidade e segurança.
Meta:	Identificar os processos críticos e disponibilizar instruções e/ou capacitar os responsáveis pela conformidade contábil, de forma que sejam cumpridos os prazos com qualidade e eficiência. Unidade: Reduzir a zero as pendências e descumprimentos de prazo.
Prazo:	2015 – Reduzir a zero as pendências e descumprimentos de prazo. 2016 – Reduzir a zero as pendências e descumprimentos de prazo. 2017 – Reduzir a zero as pendências e descumprimentos de prazo. 2018 – Reduzir a zero as pendências e descumprimentos de prazo.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CCONT – Aiche Leite Mohd Saleh

Objetivo 7.7:	Implantar Novo Procedimento para Pagamento de Faturas
Ação:	Implantar novo procedimento para pagamento de faturas, de forma que os processos de pagamento sejam apartados do processo principal.
Meta:	Identificar os processos críticos e disponibilizar instruções e/ou capacitar os responsáveis pela conformidade contábil, de forma que sejam cumpridos os prazos com qualidade e eficiência. Unidade: Implantar o novo procedimento e estabelecer ponto de controle para apurar se a nova sistemática efetivamente permitiu agilizar o processo de pagamento.
Prazo:	2015 – 100 % implantado e controlado
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CPL – Nathércia Maria Ribeiro de A.C. Meleiro

Objetivo 7.8:	Melhoria do Processo de Fiscalização de Contratos
Ação:	Implementar melhoria nos processos de fiscalização de contratos, de forma que sejam revistas e padronizadas as planilhas de controle, que devem contemplar todos os itens a serem observados, com o objetivo de minimizar eventuais riscos. Adotar outros procedimentos, que permitam a melhoria de processo, tais como: treinamentos, cartilhas, estágios, etc..
Meta:	Dispor de material de apoio padronizado e automatizado, que reduzam os riscos de eventuais erros. Unidade: 100% das planilhas revisadas e 100% funcionários envolvidos treinados.
Prazo:	2015 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados. 2016 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados. 2017 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados. 2018 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade.
Responsável	CGPOA/CFC – José Adalberto Ribeiro de Andrade

Objetivo 7.9:	Solução para Manutenção Predial
Ação:	Buscar solução para Manutenção Predial com a melhor relação custo-benefício.
Meta:	Dispor de serviços necessários à Manutenção predial, com atendimento tempestivo, de forma que sejam minimizados os riscos inerentes. Unidade: Implantar 100% da solução.
Prazo:	2015 – Implantar 100% da solução. 2016 – Implantar 100% da solução. 2017 – Implantar 100% da solução. 2018 – Implantar 100% da solução.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade.
Responsável	CGPOA/CFC - José Adalberto Ribeiro de Andrade

Objetivo 7.10:	Gerenciamento da infraestrutura tecnológica institucional
Ação:	Manter a infraestrutura de hardware atualizada e operacional para garantir o apoio tecnológico contínuo às aplicações do negócio.
Meta:	**Parque computacional crítico em produção atualizado e em garantia:** Indicador: % (percentual) do parque crítico em garantia. Métrica: 95% **Adequação e evolução da infraestrutura de armazenamento, conectividade e do parque de ativos às necessidades do ITI:** Indicador: % (percentual) de conformidade às necessidades do Instituto. Métrica: 95% de conformidade aos objetivos de negócio
Prazo:	2015, 2016, 2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA/CODIS

Objetivo 7.11:	Disponibilizar e Gerenciar softwares aplicativos em alinhamento com os requisitos do negócio
Ação:	Traduzir os requisitos de negócio em especificações de projeto para a aquisição, a manutenção e o desenvolvimento de softwares do Instituto, a fim de apoiar de forma adequada as operações do negócio, levando em consideração o direcionamento tecnológico e a arquitetura de informação.
Meta:	**Contratação de fábrica de software para manutenção e desenvolvimento de sistemas** Indicador: % (percentual) softwares desenvolvidos/mantidos Métrica: 80% de contratações de fábrica de software para manter/desenvolver os softwares priorizados pelo CETI **Manutenção dos sites do ITI** Indicador: Quantidade de sites mantidos **Aquisição de softwares aplicativos para alcançar os objetivos do negócio:** Indicador: % (percentual) de softwares aplicativos do Órgão gerenciados tecnicamente pela CGPOA/CODIS. Métrica: 60% dos softwares gerenciados pela CGPOA/CODIS
Prazo:	2015, 2016, 2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA/CODIS

Objetivo 7.12:	Gerenciamento da Governança de TI no âmbito da CODIS
Ação:	Analisar as tecnologias existentes e planejar qual direcionamento é apropriado para implementar a estratégia de TI e identificar quais tecnologias geram oportunidades de negócio, com a finalidade de gerar valor para o negócio e aderência a requisitos e *compliance*.
Meta:	**Adoção de um Modelo de controle para a Governança de TI:** Indicador: Quantidade de processos da CGPOA/CODIS aderentes ao COBIT. Métrica: 3 (três) objetivos de controle de Governança aderentes ao COBIT por ano. **Aplicação de um Modelo de Gerenciamento de Projetos:** Indicador: % (percentual) de projetos da CGPOA/CODIS que seguem os padrões e as práticas de gerenciamento de projetos. Métrica: 90% dos projetos da CGPOA/CODIS aderentes às boas práticas de gerenciamento de projetos. **Adoção de um modelo de melhores práticas para Gerenciamento de Serviços de TI:** Indicador: % (percentual) de serviços de TI ofertados pela CGPOA/CODIS que seguem as melhores práticas de gerenciamento de serviços. Métrica: 25% dos serviços aderentes às boas práticas de gerenciamento de projetos **Contratação de Serviços em alinhamento as necessidades organizacionais:** Indicador: Quantidade de serviços contratados. Métrica: Mínimo dois serviços contratados ou mantidos por ano.
Prazo:	2015, 2016, 2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA/CODIS

Objetivo 7.13:	Gerenciamento da segurança dos ambientes físico e lógico da CODIS
Ação:	Manter os ativos e processos internos aderentes à legislação de segurança vigente.
Meta:	**Alinhamento com Política de Segurança da Informação e Comunicações (POSIC) e às Normas Complementares do Gabinete de Segurança Institucional (NC/GSI):** Indicador: Quantidade de ações/rotinas aderentes à POSIC e às NC/GSI. Métrica: 25 ações/rotinas aderentes à POSIC e às NC/GSI **Garantir a disponibilidade dos ativos críticos gerenciados** Indicador: Tempo de indisponibilidade devido a incidentes no ambiente físico e lógico Métrica: Tempo de indisponibilidade dos ativos críticos < 0,5 % **Garantir a confidencialidade, autenticidade, integridade e controle de acesso das informações críticas** Indicador: Quantidade de incidentes causados por falhas ou violação da segurança Métrica: Incidentes causados por falhas ou violação da segurança < 5 por ano
Prazo:	2015, 2016, 2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA/CODIS

Objetivo 7.14:	Promover estudos e submeter à aprovação das Autoridades Competentes proposta de reestruturação organizacional do ITI, adequada às suas responsabilidades institucionais
Ação:	Acompanhar aprovação junto ao MPOG do processo de carreira do ITI. Encaminha proposta consolidada do regimento interno para aprovação.
Meta:	Aprovação de concurso para quadro próprio. Contratação de aprovados no concurso.
Prazo:	2015, 2016, 2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA -

Objetivo 7.15:	Implementar gestão com vistas a aquisição de sede própria e/ou melhoramento nas instalações atuais.
Ação:	Criar GT para propor alternativas para a sede própria.
Meta:	Dispor de sede própria ou melhorias nas instalações atuais.
Prazo:	2015, 2016, 2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA -

8. Reestruturação Orçamentária

Objetivo 8.1:	Melhoria da Gestão de Orçamento e Execução Financeira
Ação:	Aperfeiçoamento da Gestão Conjunta do Orçamento e da Execução Financeira do Instituto, com vistas à otimização do relacionamento com Setorial.
Meta:	Maximização do uso dos recursos orçamentários – Unidade: percentual de utilização dos recursos
Prazo:	2015 – 95% 2016 – 95% 2017 – 95% 2018 – 95%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CPO e CGPOA/COF – Maria Izilda Ferreira e Joseni A Belmiro de A. Silva

9. Monitoramento de Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP Brasil.

Objetivo 9.1:	Monitorar Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP Brasil.
Ação:	Conhecer, acompanhar, prestar apoio técnico para que os Projetos de Lei que envolvam assinaturas eletrônicas e a prestação de serviços de certificação digital contribuam para a massificação do uso da certificação digital da ICP Brasil.
Meta	Contribuir para a Massificação da Certificação Digital ICP Brasil.
Prazo:	2015, 2016, 2017 e 2018 (continuado)
Recursos Orçamentários	Ação orçamentária 2000 – Administração da Unidade
Responsável:	Gabinete

ANEXO 2

RESULTADOS DO PLANEJAMENTO ESTRATÉGICO 2017

PLANEJAMENTO ESTRATÉGICO

ACOMPANHAMENTO DAS AÇÕES

Exercício 2017

ITI
Instituto Nacional de Tecnologia da Informação

SUMÁRIO

FATO RELEVANTE

O quadro diretivo do Instituto Nacional de Tecnologia da Informação – ITI foi alterado a partir de 28 de abril de 2017, passando a ser composto pelos seguintes membros:

Gastão José de Oliveira Ramos

Diretor-Presidente

Waldeck Pinto de Araújo Júnior

Diretor de Infraestrutura de Chaves Públicas

Rafaelo Abritta

Diretor de Auditoria, Normalização e Fiscalização

Ronoilton Gonçalves

Coordenador Geral de Planejamento, Orçamento e Administração – CGPOA

Alexandre Munia Machado

Procurador-Federal - Chefe

APRESENTAÇÃO

O **Instituto Nacional de Tecnologia da Informação – ITI** (www.iti.gov.br) é uma Autarquia Federal, criada por intermédio do Art. 12 da Medida Provisória n° 2.200, de 24 de agosto de 2001, com sede e foro no Distrito Federal, com Estrutura Regimental aprovada pelos Decretos n° 8.985, de 8 de fevereiro de 2017 e n° 9.183, de 30 de outubro de 2017, vinculada à Casa Civil da Presidência da República, na forma do Decreto n° 8.872, de 10 de dezembro de 2016, com a finalidade de ser a Autoridade Certificadora Raiz – AC da Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

Sua competência principal é operacionalizar, manter e modernizar a Infraestrutura de Chaves Públicas, sendo a primeira Autoridade da Cadeia de Certificação Digital – AC Raiz.

O ITI também tem atribuição de estimular e articular projetos de pesquisa científica e desenvolvimento tecnológicos voltados à ampliação da cidadania digital, bem como a popularização da certificação digital e inclusão digital, atuando sobre questões como sistemas criptográficos, hardwares compatíveis com padrões abertos e universais, convergência digital de mídias, entre outras.

CERTIFICAÇÃO DIGITAL

A Medida Provisória 2.200-2, de 24 de agosto de 2001, deu início à implantação do sistema nacional de certificação digital da Infraestrutura de Chaves Pública Brasileira – ICP – Brasil, criada com o objetivo de regulamentar a utilização da Certificação Digital no País.

O Certificado Digital funciona como uma carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação realizada nos meios virtuais, como a rede de computadores – Internet. Tecnicamente, o certificado é um documento eletrônico que por meio de procedimentos lógicos e matemáticos assegura a integridade das informações e a autoria das transações.

O Certificado Digital contem dados de seu titular, tais como, nome completo, data de nascimento, CPF, número da identidade, assinatura da Autoridade Certificadora que o emitiu, entre outros atributos, conforme consta na Política de Segurança de cada Autoridade Certificadora.

Portanto, quando se utiliza um certificado digital para gerar um documento eletrônico, inicia-se uma verificação dos dados e da validade do certificado, cujo processo se vale de chaves criptográficas criadas mediante o uso de matemática avançada. A cada entidade (pessoa ou empresa) é associada um par de chaves criptográficas, cuja verificação ou certificação *on line* é feita pela Autoridade

Certificadora que o emitiu.

A Certificação Digital confere segurança e validade jurídica a transações realizadas de forma virtual, ou seja, sem presença física do interessado, mas que exigem a identificação inequívoca da pessoa que está assinando o documento ou transação de forma eletrônica.

A certificação digital é uma ferramenta que garante integridade, autenticidade, segurança e validade jurídica aos atos praticados com seu uso, por essa razão é muito utilizada em operações de comércio eletrônico, assinatura de contratos, operações bancárias, iniciativas de governo eletrônico, diversas transações da Receita Federal e de comércio exterior, dentre muitas outras.

O Brasil conta com uma infraestrutura pública, mantida e auditada por um órgão público, no caso o Instituto Nacional de Tecnologia da Informação – ITI, a quem compete executar as políticas de certificação e as normas técnicas e operacionais estabelecidas pelo Comitê Gestor da ICP – Brasil, bem como realizar os processos de credenciamento, fiscalização e auditoria das entidades que compõem a ICP – Brasil, com o objetivo de manter a qualidade dos serviços prestados e o nível de confiança que a sociedade deposita na infraestrutura.

O ITI atua também como Secretaria-Executiva do Comitê Gestor da ICP – Brasil, composto por representantes dos seguintes Órgãos: Casa Civil da Presidência da República, Gabinete de Segurança Institucional da Presidência da República, Ministério da Justiça e Segurança Pública, Ministério da Indústria, Comércio Exterior e Serviços, Ministério do Planejamento, Desenvolvimento e Gestão, Ministério da Ciência, Tecnologia, Inovações e Comunicações e Ministério da Fazenda, ANCD – Associação Nacional de Certificação Digital, Câmara e-Net – Câmara Brasileira de Comércio Eletrônico, AARB – Associação das Autoridades de Registro do Brasil, CNC – Confederação Nacional do Comércio de Bens, Serviços e Turismo e FEBRABAN – Federação Brasileira de Bancos.

O ITI é responsável pela condução da seguinte ***Iniciativa***, no âmbito do PPA 2016-2019:

2038 - Programa Democracia e Aperfeiçoamento da Gestão Pública

1158 - Objetivo: Aumentar a eficiência da ação do Estado mediante o uso integrado da tecnologia da informação e o aprimoramento da gestão, contribuindo para segurança da informação e comunicações e a segurança cibernética.

06LB - Iniciativa: Massificação e Aperfeiçoamento da Certificação Digital ICP – Brasil e outras tecnologias de segurança da informação e identificação digital, necessárias às transações eletrônicas de interesse da União, dos Estados, dos Municípios, do Distrito Federal e da Sociedade, mediante a garantia de pleno funcionamento da Infraestrutura de Chaves Públicas Brasileira e do Carimbo do Tempo da ICP – Brasil.

DIRETRIZES ESTRATÉGICAS

A análise ambiental evidenciou a necessidade de atuação em determinadas frentes, cujo êxito é considerado fundamental para o cumprimento da missão e o alcance da visão do Instituto Nacional de Tecnologia da Informação - ITI.

A partir desse diagnóstico foram traçadas as seguintes **Diretrizes Estratégicas:**

1. Operacionalização, Manutenção e Modernização do Sistema Nacional de Certificação Digital – ICP – Brasil;

2. Auditoria e Fiscalização do Sistema Nacional de Certificação Digital da ICP – Brasil;

3. Normatização e Pesquisa em Criptografia e Segurança da Informação;

4. Prospecção e Evolução Tecnológica em Criptografia e Segurança da Informação;

5. Fomento a aplicações com uso da Certificação Digital ICP – Brasil;

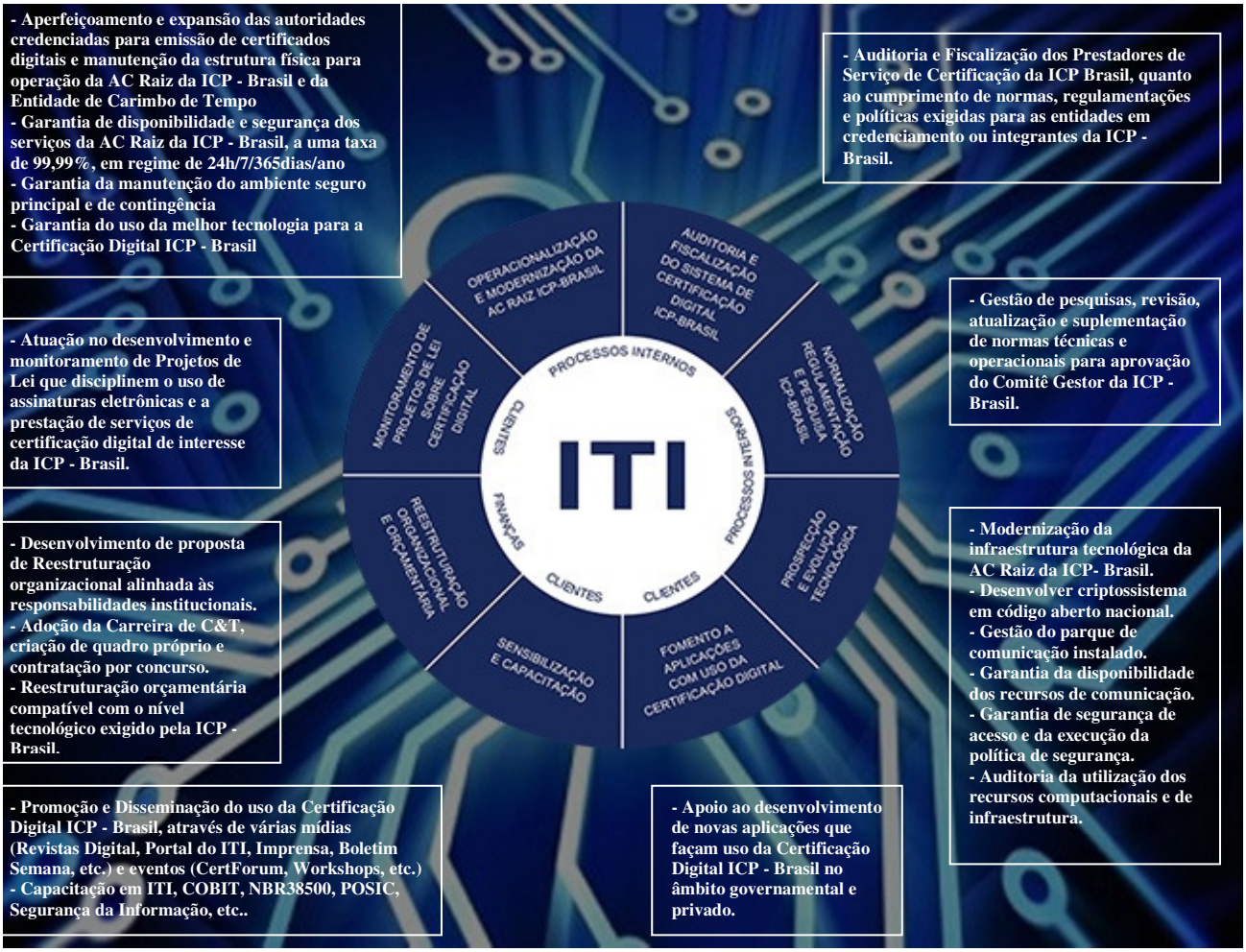
6. Promoção e Disseminação do Uso da Certificação Digital ICP – Brasil: Sensibilização e Capacitação;

7. Macroprocessos de Apoio e Reestruturação Organizacional;

8. Reestruturação Orçamentária

9. Monitoramento de Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP Brasil.

As Diretrizes e Ações Estratégicas foram consubstanciadas no Mapa Estratégico abaixo:



ACOMPANHAMENTO DAS AÇÕES ESTRATÉGICAS EXERCÍCIO – 2017

Informamos abaixo os resultados obtidos em cada uma das ações estratégicas no primeiro semestre do exercício de 2017:

1. Operacionalização, Manutenção e Modernização do Sistema Nacional de Certificação Digital ICP – Brasil.

Objetivo 1.1:	Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil
Ação:	Aperfeiçoamento e expansão das Autoridades Credenciadas para emissão de certificados digitais e manutenção da estrutura física para operação da AC Raiz da ICP – Brasil e da Entidade de Carimbo de Tempo
Meta:	Manutenção de dois Centros de Certificação Digital (principal e contingência)
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável	CGO – André Machado Caricatti
Resultados - 2017	**1º Semestre de 2017** Registraram-se avanços nas seguintes frentes: a) Criação da Autoridade Certificadora-Raiz na Cadeia v5 – RSA – 4096 bits; b) Alteração do intervalo de emissão da Lista de Certificados Revogados na Cadeia v3. Intervalo este com data limite até expiração da referida Autoridade Certificadora Raiz – cadeia v3. c) Assinatura de Certificados Digitais da AC-Serasa ACP e AC Certisign, ambas de Primeiro Nível – na cadeia v5; d) Aperfeiçoamento do sistema de gerenciamento de certificado digital – SCG Ywapa(Simétrico) – Objetivo: atender o Sistema Biométrico da ICP - Brasil; e) Execução do Plano de Teste de Versões referentes ao SGC Ywapa – Simétrico. f) Solicitação à Contratada – Kryptus - em alterar o firmware do Módulo Criptográfico para assinatura de Chaves Simétricas. g) Elaboração dos seguintes Planos de Testes: Sistema de Gerenciamento de Certificados – SGC Ywapa e Módulo Criptográfico – ASI HSM. h) Implementação do Ambiente de Teste da ICP -Brasil – Cadeia v5 no laboratório da CGO/DINFRA; i) Emissão da Lista de Certificados Revogados – LCRs. j) Condução do Grupo de Trabalho – GT 2 - Tema: Novos Algorítmos – Curvas Elípticas, Resumos Criptográficos – HASH e Plataforma Criptográfica – *Middleware*. **2º Semestre de 2017** Quanto à operação da AC - Raiz da ICP - Brasil, destacaram-se as seguintes atividades: a) Assinatura do Certificado Digital de primeiro nível da AC Defesa e da AC SAFEWEB; b) Exportação da Chave Criptográfica Simétrica das seguintes Autoridades Certificadoras: AC IMESP e AC Digital Sign; c) Emissão das LCRs cadeias v1, v2, v4 e v5 no ambiente de Contingência e Produção; e d) Assinatura e publicação das Listas de Políticas de Assinaturas nos padrões – XADES, CADES, PADES. Quanto à Entidade de Auditoria de Tempo, foram renovados os Certificados de Alvarás, Certificado de Conexão e de Autenticação de três Sistema de Auditoria de Sincronismo de Tempo -TSMCs.

Objetivo 1.2:	Manter ambiente seguro principal para a AC Raiz
Ação:	Manter a estrutura física para operação da AC Raiz da ICP – Brasil e Entidade de Auditoria de Tempo
Meta	Contratação de empresa especializada para a manutenção preventiva e corretiva dos subsistemas do ambiente seguro. Contratação dos meios físicos e lógicos para acesso à Internet. Contratação dos meios físicos e lógicos de contingência para o acesso à Internet. Garantir a disponibilidade de 99,99%, conforme legislação vigente.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior
Resultados - 2017	Para garantir a disponibilidade de 99,99% e pleno funcionamento da AC Raiz, são mantidos 2 (dois) Centros de Certificação Digital – CCD, sendo um em Brasília/DF (ambiente seguro principal), nas instalações da Presidência da República, e outro em Florianópolis/SC, na Universidade Federal de Santa Catarina - UFSC. Ambos os CCD são compostos de sistemas redundantes e autônomos, compostos dos seguintes subsistemas:

- Subsistema de Alimentação Elétrica;
- Subsistema de Climatização;
- Subsistema de Detecção e Combate a Incêndio;
- Subsistema de Supervisão e Controle;
- Subsistema de Controle de Acesso e Vigilância.

Em virtude da alta disponibilidade exigida pelas normas da ICP - Brasil (99,99%) é necessário manter contrato com empresa especializada para manutenção preventiva e corretiva dos subsistemas descritos acima, que são monitorados em regime 24x7 por equipe especializada. Além disso, faz-se necessário e são mantidos contratos para prestação de serviço de provimento dos meios físicos e lógicos para acesso à Internet.

No ambiente seguro principal da AC Raiz, são mantidas duas infraestruturas de rede e internet completamente independentes entre si e também independentes daquela do ambiente seguro de contingência com administração e gerenciamento realizados pelos técnicos do próprio ITI. Em tal ambiente, são mantidos a Entidade de Auditoria do Tempo – EAT, os repositórios da AC Raiz – parte online disponível para acesso através da Internet – onde são disponibilizados os certificados emitidos, as Listas de Certificados Revogados (LCR) e políticas de assinaturas. Essas informações são disponibilizadas nos dois sítios de Internet no CCD de Brasília/DF e, ainda, em um terceiro em Florianópolis/SC (contingência).

A fim de atender à disponibilidade prevista nos normativos, os serviços são disponibilizados em servidores redundantes que respondem pelo mesmo domínio "acraiz.icpbrasil.gov.br", em 03 (três) infraestruturas distintas, conforme descrito acima, de forma que somente haverá indisponibilidade quando todos os servidores/informação estiverem simultaneamente indisponíveis. Havendo a indisponibilidade de alguma infraestrutura, o serviço sofrerá degradação no acesso proporcional ao número de servidores/informações indisponíveis, porém o conteúdo manter-se-á acessível.

No exercício de 2017, foi possível garantir a disponibilidade do Sistema de Certificação Digital e da Entidade de Auditoria do Tempo – EAT da ICP - Brasil, na taxa mínima de 99,99% prevista, conforme exige a legislação vigente.

Para tanto, foi contratada empresa especializada para manutenção preventiva e corretiva dos subsistemas do ambiente seguro e foram contratados os meios físicos e lógicos para acesso à Internet para o ambiente principal.

No exercício destacaram-se ainda as seguintes realizações:

a) **Aquisição de *Storages***: Foi realizada a aquisição de uma nova solução de armazenamento (storage) para a AC Raiz composto de dois equipamentos (um para o ambiente de produção e outro para o ambiente de contingência) que, além de tecnologicamente mais modernos que os atuais, dobram a capacidade de armazenamento e, ainda, permitem expansão, caso necessário;

b) **Contratação de Manutenção dos Servidores**: Foi contratada a manutenção do parque de servidores de rede, que se encontravam fora da garantia do fabricante, trazendo uma maior segurança para os ambientes tecnológicos da AC Raiz;

c) **Contratação de Manutenção das Bibliotecas de Fitas**: Foi contratada a manutenção das bibliotecas de fitas (robôs de backup), que se encontravam fora da garantia do fabricante, trazendo uma maior segurança para o sistema de armazenamento de longo prazo das informações dos ambientes da AC Raiz;

d) **Aquisição de Servidores:** Foram adquiridos novos servidores de rede, tecnologicamente mais modernos que os atuais, permitindo uma expansão na capacidade de provimento de serviços nos ambientes da AC Raiz;

e) **Aquisição de Solução de Virtualização**: Foi adquirida solução de virtualização (VMWare) para os ambientes da AC Raiz, uma vez que utilizávamos a versão *freeware*, disponibilizando, a partir de agora, de novos recursos como: melhor utilização dos recursos de hardware disponíveis, melhor gerenciamento do parque de servidores de rede e diminuição do tempo de indisponibilidades de serviços.

Objetivo 1.3:	Manter ambiente seguro de contingência para a AC Raiz
Ação:	Manter estrutura física de contingência para operação da AC Raiz da ICP – Brasil e Entidade de Carimbo de Tempo
Meta:	Prover estrutura física de contingência para operação da AC Raiz da ICP – Brasil e Entidade de Auditoria de Tempo. Contratação de hospedagem do ambiente de contingência para a Autoridade Certificadora Raiz e da Entidade de Auditoria de Tempo da ICP – Brasil. Contratação dos meios físicos e lógicos para o acesso à Internet do ambiente de contingência. Contratação dos meios físicos e lógicos de contingência para o acesso à Internet do ambiente de contingência. Garantir a disponibilidade de 99,99%, conforme legislação vigente.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior
Resultados - 2017	Para garantir a contingência da infraestrutura e das chaves criptográficas e o pleno funcionamento da AC Raiz, são mantidos 2 (dois) Centros de Certificação Digital - CCD, sendo um em Brasília/DF e outro em Florianópolis/SC, este denominado ambiente seguro de contingência para a AC Raiz. Ambos os CCD são compostos de sistemas redundantes e autônomos, compostos dos seguintes subsistemas: − Subsistema de Alimentação Elétrica; − Subsistema de Climatização; − Subsistema de Detecção e Combate a Incêndio; − Subsistema de Supervisão e Controle; − Subsistema de Controle de Acesso e Vigilância. Em virtude da alta disponibilidade exigida pelas normas da ICP - Brasil (99,99%) é necessário manter contrato com empresa especializada para manutenção preventiva e corretiva dos subsistemas descritos acima. Assim, o ITI mantém um acordo de cooperação (TC n° 01/2013), vigente até 31/12/2017, com a Universidade Federal de Santa Catarina - UFSC que é responsável pela operação do ambiente seguro de contingência da AC Raiz da ICP - Brasil, pela contratação de empresa especializada para manutenção preventiva e corretiva dos subsistemas, pela monitoração do ambiente em regime de 24 horas x 7 dias por equipe especializada, além dos serviços para provimento dos meios físicos e lógicos para acesso à Internet. No ambiente seguro de contingência da AC Raiz, é mantida uma infraestrutura de rede e internet completamente independente do ambiente seguro principal com administração e gerenciamento do repositório da AC Raiz e do repositório das políticas de assinatura da ICP – Brasil, realizados pelos técnicos do próprio ITI. Em tal ambiente é mantido, além da contingência da Entidade de Auditoria do Tempo – EAT, o repositório da AC Raiz – parte online disponível para acesso através da Internet – onde são disponibilizados os Certificados, as Listas de Certificados Revogados (LCR) e políticas de assinaturas. Essas informações são disponibilizadas em um sítio de Internet no CCD de Florianópolis/SC, além dos dois outros disponibilizados nos sítios de Internet do CCD de Brasília/DF (ambiente principal). No exercício de 2017, foi possível garantir a disponibilidade do Sistema de Certificação Digital e da Entidade de Auditoria do Tempo – EAT da ICP – Brasil, na taxa mínima de 99,99%, conforme exige a legislação vigente. Para tanto, foi mantido o acordo de cooperação (TC n° 01/2013) com a UFSC para a operação e manutenção do ambiente seguro de contingência da AC Raiz da ICP - Brasil, bem como o provimento dos serviços necessários para acesso à Internet.

Objetivo 1.4:	Modernizar os subsistemas do ambiente seguro do ITI
Ação:	Manter os subsistemas do ambiente seguro da AC Raiz atualizados.
Meta	Adequar os subsistemas, mantendo a garantia e suporte continuados dos fabricantes e/ou empresa especializada: - Adequação e atualização tecnológica do subsistema de climatização - Adequação e atualização tecnológica do subsistema de detecção e combate à incêndio - Adequação e atualização tecnológica do subsistema de supervisão e controle - Adequação das instalações técnicas da DINFRA e instalação de solução de operação e monitoramento remoto (NOC)
Prazo:	2017
Recursos Orçamentários	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior

Resultados - 2017	No ano de 2017, foi possível a renovação do parque de servidores, *storages,* contratação de manutenção de servidores e fitotecas e aquisição de solução de virtualização, relacionadas nos resultados do Objetivo 1.2. Por outro lado, ainda não foi possível promover as adequações tecnológicas necessárias ao ambiente seguro da AC Raiz e a instalação de NOC (Centro de Operação) em nível 3 de segurança, conforme previsto nos normativos da ICP – Brasil. Vale ressaltar, que é premente a necessidade de implantação do nível 3 de segurança na Sede do ITI, de forma que o ambiente de segurança da DINFRA esteja compatibilizado com a Sala Cofre a fim de agilizar as operações da AC Raiz e minimizar as necessidades de deslocamentos para acesso físico ao ambiente seguro, uma vez que a atual estrutura exige que determinadas atividades operacionais sejam executadas apenas naquele ambiente.

Objetivo 1.5:	Prover Infraestrutura para operação da Entidade de Carimbo do Tempo
Ação:	Manter hardware e software para operação da Entidade de Carimbo de Tempo
Meta:	Garantir a disponibilidade de 99,5%, conforme legislação vigente. Contratação de suporte, manutenção preventiva e corretiva para os sistemas e equipamentos Bry. Contratação de suporte, manutenção preventiva e corretiva para os sistemas e equipamentos Thales. Aquisição de infraestrutura de contingência para a Entidade de Carimbo de Tempo. Aquisição de infraestrutura de homologação para a Entidade de Carimbo de Tempo.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGO – André Machado Caricatti
Resultados - 2017	No exercício de 2017 foi mantida a disponibilidade de 99,5% do Sistema de Carimbo do Tempo. Para tanto, foi mantida a contratação de suporte, manutenção preventiva e corretiva para os sistemas e equipamentos da BRY e THALES. No período foram implementadas outras melhorias, tais como: a) Configuração do sistema monitor de rastreabilidade; b) Instalação de antena e receptor GPS no ambiente de contingência; c) Configuração dos servidores de Auditoria do Tempo, um da BRY (SAS) e um da Thales (TSMC), no ambiente de contingência.

Objetivo 1.6:	Contratar auditoria independente
Ação:	Manter certificação de operação da AC Raiz, em conformidade com os normativos vigentes.
Meta:	Manter certificação periódica emitida por terceira parte de operação da AC Raiz de acordo com os normativos.
Prazo:	2017, 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior
Resultados - 2017	O Comitê Gestor da ICP - Brasil aprovou, por meio da Resolução nº 106, de 25 de agosto de 2015, a contratação de empresa de auditoria independente para auditar anualmente o ambiente operacional da Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviço de suporte, segundo as normas e padrões estabelecidos para própria ICP - Brasil e, ainda, segundo os normativos internacionais *WebTrust*, nos exercícios de 2015 a 2019. No exercício de 2017 a auditoria foi realizada pela empresa de auditoria independente *Ernest & Young* e abrangeu os ambientes operacionais da AC Raiz e seu Prestador de Serviço de Suporte. Pela primeira vez, a AC Raiz da ICP – Brasil recebeu um parecer com conceito 'adequado', ou seja, com ausência de não-conformidades de acordo com ADE-ICP-08.F (http://www.iti.gov.br/images/repositorio/legislacao/adendos/ADE-ICP-08-F-v-1.0-Conceitos.pdf), além do selo Webtrust referente ao período de 09 de setembro de 2016 a 08 de setembro de 2017, disponível em (https://cert.webtrust.org/ViewSeal?id=2378).

Objetivo 1.7:	Aperfeiçoar o processo de identificação do sistema ICP - Brasil
Ação:	Mitigar os riscos decorrentes das fragilidades no processo de identificação do Sistema Nacional de Certificação Digital ICP - Brasil.
Meta:	Propor e implementar melhorias no sistema de identificação para mitigar os riscos decorrentes das fragilidades identificadas.
Prazo:	2017
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	Gabinete – Eduardo Magalhães de Lacerda Filho

Resultados - 2017	O sistema anti-fraude (SAF) passou a operar em todos os pontos de atendimento da ICP - Brasil. Todas as Autoridades de Registro comunicam as fraudes e tentativas de fraudes às suas respectivas Autoridades Certificadoras, por meio de um módulo de comunicação digital, e essas repassam a informação para o ITI, que possui um módulo/servidor centralizado de todas as comunicações. O sistema está 100% operacional. O sistema anti-fraude (SAF) fornecerá a lista negativa biométrica dos Prestadores de Serviço Biométrico (PSBio). O Comitê Gestor da ICP - Brasil prorrogou o prazo para entrada do sistema biométrico da ICP - Brasil para o dia 02/02/2018. Foram credenciados 3 PSBios e mais dois estão em análise. Testes de homologação estão sendo feitos para viabilidade normativa.

Objetivo 1.8:	Fomentar o sistema de Homologação da ICP - Brasil
Ação:	Manter um sistema de homologação de hardware para a ICP - Brasil propiciando a migração para o sistema SBAC
Meta	Propiciar a migração do sistema de homologação ICP - Brasil para o INMETRO (SBAC) propiciando o reconhecimento internacional das certificações emitidas.
Prazo:	2017
Recursos Orçamentários	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGO – André Machado Caricatti
Resultados - 2017	**1º Semestre de 201**7 No âmbito do Sistema de Homologação da ICP-Brasil, foram homologados os seguintes produtos: a) Leitor/Gravador de Cartão Inteligente, Modelo "SCR 3310 V2.0 RD1-X" - CIS Eletrônica da Amazônia Ltda., em 13/02/2017; b) Leitor/Gravador de Cartão Inteligente, Modelo "IDBridge CT30" – GEMALTO, em 13/02/2017; c) Cartão Criptográfico (*Smart Card*), Modelo "JCOP 2.4.2 R2" Marca NXP - Thomas Greg & Sons, Gráfica e Serviços, Indústria e Comércio, Importação e Exportação Ltda, em23/03/2017; d*) Token* Criptográfico, Modelo "*eToken* 5110" Marca Safenet Gemalto - SafeNet Tecnologia em Informática Ltda., em 05/04/2017; e) Cartão Criptográfico – marca Safenet Gemalto, em 24/10/2017; f) Módulo de Segurança Criptográfico da marca Safenet Gemalto, em 26/12/2017. Registre-se que as homologações foram realizadas segundo as regras anteriores aos prazos estabelecidos pelo INMETRO para nova creditação de produtos.

2. Auditoria e Fiscalização do Sistema Nacional de Certificação Digital da ICP - Brasil

Objetivo 2.1:	4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Ação:	Certificar, por meio de auditorias e fiscalizações operacionais e de credenciamento, a conformidade dos processos, procedimentos operacionais e atividades dos prestadores de serviço de certificação, com as suas respectivas declarações de prática de certificação, suas políticas de certificação, a política de segurança e demais documentos, regulamentações e normas gerais estabelecidos para as entidades em credenciamento ou integrantes da ICP – Brasil, por meio de processo de auditoria e fiscalização consubstanciados em relatórios, devendo as irregularidades serem acompanhadas até sua correção.
Meta	100 relatórios de auditoria e fiscalização/ano
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Responsável:	CGAF – Pedro Pinheiro Cardoso
Resultados - 2017	As atividades de Auditoria e Fiscalização dos Provedores dos Serviços de Certificação Digital tem por objetivo verificar o cumprimento das políticas, diretrizes e normas definidas pelo Comitê Gestor da ICP - Brasil (CG/ICP-Brasil). Essas ações são divididas em: Auditorias Pré-operacionais e Operacionais, Fiscalizações e Análise, Avaliação de aprovação de relatórios de auditorias realizadas por terceiros, que juntas proporcionam a elevação dos níveis de qualidade e dos níveis de segurança nas operações eletrônicas e processos manuais, através da verificação dos procedimentos operacionais e tecnológicos adotados pelos PSC's. ***Descrição de Objetivos e Metas*** Para o exercício de 2017 foram estabelecidas as seguintes metas de auditorias e fiscalizações nos Prestadores de Serviço de Certificação – PSC, com o objetivo de transmitir confiança à comunidade de usuários dos serviços de Certificação Digital no Brasil:

TIPODEATIVIDADE(A)	PREVISTO(B)	REALIZADO(C)	(C/B)
AuditoriaOperacionalemAC	14	03	21%
Auditoria Pré-operacional em AC e PSBIO	04	19	475%
Auditoria Pré-operacional de ACT	01	0	0%
Fiscalizações em AC	07	07	100%
Fiscalizações em AR	13	16	123%
Análise de Credenciamento de AR	80	146	182%
Credenciamento de Empresas de Auditoria	01	01	100%
TOTAL	**120**	**192**	**160%**

As auditorias pré-operacionais são realizadas sob demanda, conforme são solicitados os credenciamentos desses PSC na ICP - Brasil, já as auditorias operacionais anuais em AC de 1°. nível são agendadas anualmente e revisadas trimestralmente e as fiscalizações realizadas a qualquer tempo.

O crescimento da Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil no exercício de 2017 foi o seguinte:

Evolução da ICP – Brasil

Quantidade de Certificados Emitidos – Janeiro a Dezembro/2017

Mês Referência	Qtde Total Certificados Emitidos
Janeiro	276.672
Fevereiro	267.164
Março	332.962
Abril	245.768
Maio	377.097
Junho	295.818
Julho	303.755
Agosto	323.479
Setembro	282.684
Outubro	303.542
Novembro	309.861
Dezembro	279.493
TOTAL	**3.598.295**

Fonte: ITI Jan-Dez/2017

Entidades Credenciadas na ICP – Brasil

ENTIDADES CREDENCIADAS	2016	2017	CRESCIMENTO %
Autoridades Certificadoras	72	91	26%
Autoridade de Registro - AR	565	658	16%
Instalações Técnicas Físicas	1.961	1.911	-0,3%
Total	**2.598**	**2.660**	**2,39%**

Fonte: ITI – Jan-Dez/2017

3. Normalização e Pesquisa em Criptografia e Segurança da Informação

Objetivo 3.1:	Normalização e Pesquisa
Ação:	Realizar pesquisas e propor a revisão, atualização e suplementação das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP – Brasil, observados os demais aspectos jurídicos sobre a matéria, com vistas a garantir a adoção de padrões de interoperabilidade e segurança compatíveis com as normas brasileiras e internacionais.
Meta	- revisão normativa da ICP - Brasil a fim de adequar-se aos regulamentos e normas internacionais (quando aplicáveis) sobre certificação digital e assuntos correlatos; - consolidação do padrão de assinatura PAdES; - consolidação do conjunto normativo dos MCT para atender ao novo processo de homologação via SBAC/INMETRO (2016); - definição dos diversos OIDs; e - emissão e gerenciamento de PAs e LPA.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 4912 – Auditoria e Fiscalização das Entidades Prestadoras de Serviços de Certificação
Responsável:	CGNP – Wilson Roberto Hirata
Resultados - 2017	A Coordenação-Geral de Normalização e Pesquisa (CGNP) realiza trabalhos de revisão, manutenção e proposição de normas técnicas e operacionais relacionadas à Infraestrutura de Chaves Públicas Brasileiras (ICP - Brasil). Nesse sentido, constantemente estuda e acompanha os padrões, regulamentos, recomendações e especificações nacionais e internacionais relacionadas à ICP - Brasil. No primeiro semestre de 2017 não houve reunião do Comitê Gestor da ICP – Brasil. No segundo semestre foram realizadas 03 reuniões presencias e 03 plenárias virtuais, resultando na publicação de 16 resoluções, conforme relação a seguir: 1. **Resolução nº 119, de 06 de julho de 2017** - Aprova a obrigatoriedade de realização de auditorias *Webtrust* para Autoridades Certificadoras – ACs que emitem certificados para usuários finais e de implementação de respostas OCSP para ACs que emitem certificados do tipo SSL/TLS nas cadeias de certificado digital ICP - Brasil. 2. **Resolução nº 120, de 06 de julho de 2017** - Altera os artigos 4º, 10 e 11 e inclui o artigo 14-A, do Regimento Interno do Comitê Gestor da ICP-Brasil. 3. **Resolução nº 121, de 06 de julho de 2017 -** Aprova os procedimentos para emissão de certificados digitais para servidores públicos da ativa e militares da União. 4. **Resolução nº 122, de 06 de julho de 2017 -** Aprova a prorrogação dos prazos de adequação das entidades ao Sistema Biométrico da ICP -Brasil. 5. **Resolução nº 123, de 06 de julho de 2017 -** Atualiza os padrões e algoritmos criptográficos da ICP - Brasil, os requisitos mínimos para as políticas de certificado na ICP - Brasil e os procedimentos para gerenciamento da chave simétrica para geração de IDN.

6. **Resolução nº 124, de 13 de setembro de 2017 -** Altera a Configuração do Propósito de Uso Para Certificados do Tipo a CF-e-SAT**.**
7. **Resolução nº 125, de 13 de setembro de 2017 -** Aprova Ajustes Redacionais No DOC-ICP-03.
8. **Resolução nº 126, de 13 de setembro de 2017 -** Aprova Ajustes Redacionais No DOC-ICP-09.
9. **Resolução nº 127, de 13 de setembro de 2017 -** Aprova a Versão 3.1 do DOC-ICP-10 - Regulamento Para Homologação de Sistemas e Equipamentos de Certificação Digital No Âmbito da ICP - Brasil.
10. **Resolução nº 128, de 13 de setembro de 2017 -** Aprova a Obrigatoriedade de Implementação da *Extensão Subject Alternative Name* para Certificados do Tipo SSL/TLS.
11. **Resolução nº 129, de 13 de setembro de 2017 -** Aprova o Relatório de Auditoria Independente Realizada No Ambiente Operacional da Autoridade Certificadora Raiz (AC RAIZ) e Seu Prestador.
12. **Resolução nº 130, de 19 de setembro de 2017 -** Institui as instalações técnicas secundárias, disciplina os procedimentos de validação externa no âmbito da ICP - Brasil e dá outras providências.
13. **Resolução nº 131, de 10 de novembro de 2017 -** Inclui itens no DOC-ICP-05, versão 4.3, no DOC-ICP-05.02, versão 1.5 e dá outras providências.
14. **Resolução nº 132, de 10 de novembro de 2017 -** Cria o DOC-ICP-17 que institui o prestador de serviço de confiança para armazenamento de chaves privadas de usuários finais e serviços de assinatura digital no âmbito da ICP - Brasil e dá outras providências.
15. **Resolução nº 133, de 07 de dezembro de 2017 -** Altera itens do DOC-ICP-03, versão 5.2, para modificação nos procedimentos de extinção de instalação técnica de ar e descredenciamento de AR e PSS.
16. **Resolução nº 134, de 07 de dezembro de 2017 -** Altera itens do DOC-ICP-03, versão 5.2, para modificação nos critérios para abertura e encerramento de posto provisório.

Em 2017 foram aprovadas pelo Diretor-Presidente do ITI, que também exerce a função de Secretário-Executivo do Comitê Gestor da ICP – Brasil, e publicadas sob responsabilidade da CGNP 11 Instruções Normativas, que suplementam as regulamentações aprovadas pelo Comitê Gestor da ICP - Brasil. Essas normas são elaboradas e/ou atualizadas pela CGNP, a saber:

1. **IN nº 01-2017, de 19 de janeiro de 2017** - Altera parâmetro em biometria, esclarece codificação de município e UF para localidades no exterior definida no artigo 1° da IN n°14.
2. **IN n° 02-2017, de 08 de fevereiro de 2017** - Complementa as informações que as ACs emissoras de certificados para usuários finais devem encaminhar ao ITI.
3. **IN Nº 03-2017, de 23 de fevereiro de 2017** - Aprova a versão 7.3 do documento requisitos das políticas de assinatura digital na ICP - Brasil (DOC-ICP-15.03).
4. **IN Nº 04-2017, de 014 de março de 2017** - Complementa as informações sobre o agente de registro que as ACs emissoras de certificados para usuários finais devem encaminhar ao ITI. (REVOGADA)
5. **IN Nº 05-2017, de 19 de junho de 2017** - Atualiza os formatos e padrões das mensagens para os serviços do diretório de registros biométricos da ICP - Brasil.
6. **IN n° 06-2017, de 11 de agosto de 2017** - Disposições para validação de solicitação de certificados para servidores públicos da ativa e militares da União.
7. **IN nº 07-2017, de 21 de agosto de 2017** - Aprova a versão 4.2 do manual de conduta técnica 1 (MCT - 01) requisitos, materiais e documentos técnicos para homologação de cartões criptográficos (*smart cards*) no âmbito da ICP - Brasil.
8. **IN nº 08-2017, de 26 de setembro de 2017** - Aprova novas versões dos manuais de conduta técnica MCT 02 - requisitos, materiais e documentos técnicos para homologação de leitoras de cartões inteligentes no âmbito da ICP - Brasil, MCT 03 - requisitos, materiais e documentos técnicos para homologação de *tokens* criptográficos no âmbito da ICP - Brasil e MCT 07 - requisitos, materiais e documentos técnicos para homologação de módulos de segurança criptográfica (MSC) no âmbito da ICP - Brasil**.**
9. **IN nº 09-2017, de 13 de novembro de 2017 -** Institui cadastro de agente de registro da ICP - Brasil, aprova seu manual de instrução e dá outras providências**.**
10. **IN nº 10-2017, de 15 de dezembro de 2017 -** Cria o DOC-ICP-17.01 - procedimentos operacionais mínimos para os prestadores de serviço de confiança da ICP - Brasil**.**
11. **IN nº 11-2017, de 18 de dezembro de 2017 -** Altera itens do DOC-ICP-05.03, versão 1.5, para atualização dos procedimentos para identificação biométrica na ICP -Brasil e dá outras providências**.**

Em decorrência da publicação das resoluções e instruções normativas, em 2017 a CGNP atualizou 11 (onze) DOC-ICP e editou 02 (dois) novos DOC-ICP, disponibilizados no sítio web do ITI, conforme relação abaixo:

- **DOC-ICP-01.01** - Padrões e Algoritmos Criptográficos da ICP - Brasil.
- **DOC-ICP-01.02** - Requisitos Adicionais Para Aderência Aos Programas de Raízes Confiáveis dos Fornecedores de Navegadores de Internet.
- **DOC-ICP-03** - Credenciamento das Entidades Integrantes da ICP - Brasil.
- **DOC-ICP-03.01** - Características Mínimas de Segurança para as AR da ICP - Brasil.
- **DOC-ICP-04** - Requisitos Mínimos para as Políticas de Certificado na ICP - Brasil.
- **DOC-ICP-05** - Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP - Brasil.

- **DOC-ICP-05.02** - Procedimentos para Identificação do Requerente e Comunicação de Irregularidades no Processo de Emissão de um Certificado Digital ICP - Brasil.
- **DOC-ICP-05.03** - Procedimentos para Identificação Biométrica na ICP - Brasil.
- **DOC-ICP-05.04** - Procedimentos para gerenciamento da chave simétrica para geração do IDN.
- **DOC-ICP-08** - Critérios e Procedimentos para Auditoria das Entidades Integrantes da ICP - Brasil.
- **DOC-ICP-09** - Critérios e Procedimentos para Fiscalização das Entidades Integrantes da ICP - Brasil.
- **DOC-ICP-10** - Regulamento para Homologação de Sistemas e Equipamentos de Certificação Digital no Âmbito da ICP - Brasil.
- **DOC-ICP-15.03** - Requisitos das Políticas de Assinatura Digital na ICP - Brasil.
- **DOC-ICP-17** - Requisitos mínimos para as declarações de práticas de prestador de serviço de confiança da ICP - Brasil – V.1.0 (NOVO)
- **DOC-ICP-17.01** - Procedimentos operacionais mínimos para os prestadores de serviço de confiança da ICP - Brasil – V.1.0 (NOVO)

Além disso, conforme disposto no Art. 8° do Decreto 8.985 de 8 de fevereiro de 2017, é atribuição da **DAFN** a definição dos diversos *Object Identifier* – OID. Em 2017 foram criados 41 novos OID, distribuídos em 13 novos pedidos de credenciamento de ACs ou ACTs, e 2 novos atributos, sendo 1 atributo opcional de certificado para nome social e 1 atributo obrigatório de certificado para servidor público da ativa e militar da União. A publicação dos OID é efetuada por meio do Adendo ADE-ICP-04.01, que se encontrava em sua versão 4.6, até o mês de dezembro 2017, disponibilizado no sítio do ITI.

Ainda no sítio do ITI foram disponibilizadas as seguintes publicações, com o objetivo de proporcionar transparência e esclarecimentos à sociedade e entidades envolvidas com a ICP - Brasil.

- **Nota Técnica nº 01/2017 -** Alerta sobre a revogação das políticas de assinatura prevista para 26/02/2017.
- **Nota Técnica nº 06/2017 -** Validação dos certificados digitais ICP - Brasil pelos navegadores Chrome e Firefox, em suas versões mais atuais.
- **Nota Técnica nº 34/2017 -** Orientações sobre o uso do nome social em certificados digitais ICP - Brasil.

Para ampliar a participação da sociedade na construção de propostas normativas, a CGNP conduziu a seguinte consulta pública, disponível no sítio do ITI:

- **Consulta Pública 01/2017 -** Condições de Confiabilidade das Políticas de Assinatura ICP - Brasil.

OUTRAS DEMANDAS NO ÂMBITO DA NORMALIZAÇÃO E PESQUISA

Por determinação do Comitê Gestor da ICP - Brasil, a CGNP compõe e coordena os seguintes Grupos Técnicos de Trabalho (GT):

- GT Revisão dos MCTs – em andamento, foram realizadas 18 reuniões em 2017.
- GT Permanente PBAD – em andamento, foram realizadas 23 reuniões em 2017; e
- GT Assinatura Remota e Portais de Assinatura – suspenso.

O GT Revisão dos MCTs foi criado para realizar a atualização dos manuais de conduta técnica relacionados com equipamentos de certificação digital, cuja homologação é obrigatória no âmbito da ICP - Brasil. Participam desse GT os seguintes órgãos: ITI, LSITEC, NCC e INMETRO. Em 2017 foram atualizados os seguintes manuais:

- **MCT nº 1 - Volume I** – Versão 4.2 - Requisitos, Materiais e Documentos Técnicos para Homologação de Cartões Criptográficos (*Smart Cards*) no Âmbito da ICP-Brasil.
- **MCT nº 1 - Volume II** – Versão 4.2 - Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos de Cartões Criptográficos (*Smart Cards*) no Âmbito da ICP - Brasil.
- **MCT nº 2 - Volume I** – Versão 3.1 - Requisitos, Materiais e Documentos Técnicos para Homologação de Leitoras de Cartões Inteligentes no Âmbito da ICP - Brasil.
- **MCT nº 2 - Volume II** – Versão 3.1 - Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Leitoras de Cartões Inteligentes no Âmbito da ICP - Brasil.
- **MCT nº 3 - Volume I** – Versão 3.1 - Requisitos, Materiais e Documentos Técnicos para Homologação de *Tokens* Criptográficos no Âmbito da ICP - Brasil.
- **MCT nº 3 - Volume II** – Versão 3.1 - Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de *Tokens* Criptográficos no Âmbito da ICP - Brasil.
- **MCT nº 7 - Volume I** – Versão 2.2 - Requisitos, Materiais e Documentos Técnicos para Homologação de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP - Brasil
- **MCT nº 7 - Volume II** -Versão 2.2 - Procedimentos de Ensaios para Avaliação de Conformidade

	aos Requisitos Técnicos de Módulos de Segurança Criptográfica (MSC) no Âmbito da ICP - Brasil. Por meio de Termo de Execução Descentralizada 01/2015-ITI o ITI, em cooperação com a UnB,foi desenvolvido o software *Plugin* para possibilitar a verificação de assinaturas digitais padrão PAdES ICP - Brasil pelos aplicativos leitores de arquivos no formato PDF. Após a entrega do *Plugin*, a CGNP passou a acompanhar as tratativas entre a UnB e Adobe referentes a ajustes no *subfilter.* Em junho de 2017 a CGNP finalizou o processo de prestação de contas deste projeto. Em setembro de 2017 foi realizado o registro do software Plugin PAdES ICP - Brasil junto ao Instituto Nacional da Propriedade Industrial – INPI, formalizado por um Certificado de Registro de Programas de Computador válido por 50 anos. Ainda sob demanda do CG ICP - Brasil, foram criados o GT de Assinatura Remota e Portais de Assinatura, cuja atividade foi interrompida em 2016. Não foi realizada reunião em 2017. Em relação à geração dos códigos de máquina das Listas de Políticas de Assinatura Aprovadas (LPA) para revalidação (LPAs vencem a cada noventa dias), a CGNP atuou na atualização das LPAs, disponibilizando os códigos para publicação no repositório da AC Raiz. Foram emitidas LPA em fevereiro e maio, agosto e novembro de 2017.

4. Prospecção e Evolução Tecnológica em Criptografia e Segurança da Informação

Objetivo 4.1:	Modernizar a infraestrutura tecnológica da AC Raiz da ICP – Brasil
Ação:	Prover infraestrutura de rede, armazenamento e segurança da AC Raiz com sistemas e equipamentos atualizados tecnologicamente.
Meta:	Substituir e atualizar os equipamentos de armazenamento da rede SAN em final do ciclo de vida para o ambiente principal e de contingência Aquisição de equipamentos para complementação e ampliação da infraestrutura de segurança da AC Raiz. Aquisição de equipamentos para complementação e ampliação da capacidade de balanceamento de enlaces e cargas para a infraestrutura de rede da AC Raiz. Atualização do parque tecnológico para o ambiente seguro principal e de contingência Aquisição de ferramentas para análise de mídias e sistemas. Aquisição de software de virtualização para o ambiente seguro principal/contingência.
Prazo:	2017
Recursos Orçamentários:	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGSI – José Rodrigues Gonçalves Júnior
Resultados - 2017	No decorrer de 2017 foi possível renovar o parte do parque tecnológico da AC – Raiz, como evidenciado abaixo: a) **Aquisição de *Storages***: Foi realizada a aquisição de uma nova solução de armazenamento (storage) para a AC Raiz composto de dois equipamentos (um para o ambiente de produção e outro para o ambiente de contingência) que, além se tecnologicamente mais modernos que os atuais, dobram a capacidade de armazenamento e, ainda, permitem expansão, caso necessário; b) **Contratação de Manutenção dos Servidores**: Foi contratada a manutenção do parque de servidores de rede, que se encontravam fora da garantia do fabricante, trazendo uma maior segurança para os ambientes tecnológicos da AC Raiz; c) **Contratação de Manutenção das Bibliotecas de Fitas**: Foi contratada a manutenção das bibliotecas de fitas (robôs de backup), que se encontravam fora da garantia do fabricante, trazendo uma maior segurança para o sistema de armazenamento de longo prazo das informações dos ambientes da AC Raiz; d) **Aquisição de Servidores:** Foram adquiridos novos servidores de rede, tecnologicamente mais modernos que os atuais, permitindo uma expansão na capacidade de provimento de serviços nos ambientes da AC Raiz; e) **Aquisição de Solução de Virtualização**: Foi adquirida solução de virtualização (VMWare) para os ambientes da AC Raiz, uma vez que utilizávamos a versão *freeware*, disponibilizando, a partir de agora, novos recursos como: melhor utilização dos recursos de hardware disponíveis, melhor gerenciamento do parque de servidores de rede e diminuição do tempo de indisponibilidades de serviços. Ainda que tenham sido feitas as aquisições descritas acima, não foi possível a aquisição de balanceadores de enlaces e cargas, cuja licitação foi frustrada. Assim, ainda é primordial a aquisição de tal solução, bem como a continuidade do processo de modernização da infraestrutura.

Objetivo 4.2:	Desenvolver e manter criptossistema em código aberto com tecnologia nacional
Ação:	Manter o hardware e software (SGC-Ywapa, Ywyra e Hawa) da AC-Raiz da ICP Brasil atualizados, de acordo com os requisitos operacionais e de algoritmos criptográficos.

Meta:	Produto: sistema implantado/Unidade de Medida: % de execução física/Quantidade anual: 1 Atender as demandas da ICP Brasil, conforme prazos estabelecidos. Manutenção do sistema de emissão de certificados digitais da Autoridade Certificadora Raiz (*Ywapa*). Manutenção do sistema de emissão de certificados de Autoridades Certificadoras intermediárias (*Ywyra*). Manutenção do sistema de emissão de certificados digitais para o usuário final (*Hawa*). Manutenção do hardware seguro da ICP Brasil. Manutenção do software do hardware seguro da ICP Brasil.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários:	Ação orçamentária 7264 – Desenvolver criptossistema em código aberto com tecnologia nacional
Responsável:	DINFRA – Luiz Carlos de Oliveira Porto
Resultados - 2017	O Termo de Execução Descentralizada com a UFSC para manutenção do SGC foi complementado em R$ 12.622,32 (doze mil seiscentos e vinte e dois reais e trinta e dois centavos).

5. Fomento a aplicações com uso da Certificação Digital ICP - Brasil

Objetivo 5.1:	Fomento da utilização de certificado digital nas soluções de TI utilizadas no âmbito do ITI
Ação:	Incentivar a utilização de certificação digital nos serviços prestados pela CGPOA/CODIS aos colaboradores do ITI para alinhar as soluções de TI aos mecanismos de segurança definidos pelo próprio Instituto.
Meta	**Fornecimento de soluções relacionadas com certificação digital** Indicador: quantidade de soluções de TI suportadas pela CGPOA/CODIS que utilizam tecnologia de certificação digital. Métrica: ao menos duas soluções suportadas pela CODIS a cada dois anos **Fornecimento de certificado digital aos colaboradores do Instituto.** Indicador: % de colaboradores que possuem certificado digital válido. Meta: 95% dos colaboradores devem possuir certificado digital válido.
Prazo:	2017 e 2018
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	CGPOA/CODIS
Resultados - 2017	Implantada certificação digital em 4 (quatro) soluções providas pela CODIS: Webmail ITI, Sistema Eletrônico de Informações (SEI-ITI), Serviço de Compartilhamento de Arquivos (Nuvem ITI), Ferramenta de Gestão de Projetos Corporativa (*Redmine*).

Objetivo 5.2:	Fomentar o desenvolvimento de novas aplicações que façam uso da Certificação Digital ICP - Brasil no âmbito governamental e privado.
Ação:	Incentivar e prestar apoio técnico ao desenvolvimento de novas aplicações que façam uso da Certificação Digital ICP - Brasil e os produtos associados no âmbito governamental e privado.
Meta	Manutenção do Assinador Digital de Referência (ADRB) padrão ICP - Brasil Manutenção do Sistema de Gerenciamento de Certificados de Atributos (SGCA) Desenvolvimento do *middleware* padrão ICP - Brasil Manutenção do verificador de conformidade do padrão de assinatura da ICP - Brasil Participar em fóruns, câmaras técnicas, comitês a fim de representar o ITI nos debates relacionados à certificação digital.
Prazo:	2017 e 2018
Recursos Orçamentários	Ação orçamentária 4917 – Funcionamento da Autoridade Certificadora Raiz da ICP – Brasil e da Entidade de Auditoria de Tempo
Responsável:	CGO - André Caricatti, Gabinete - Ruy Ramos

Resultados - 2017	No decorrer de 2017, o ITI licenciou o Sistema de Gerenciamento de Certificados - SGC para o Tribunal Superior Eleitoral (TSE); e também o Código de Referência do Padrão de Assinatura Digital e do Verificador de Conformidade para o Banco Central do Brasil. Foi fechado um Termo de Execução Descentralizada com a Universidade de Santa Catarina – UFSC no valor de R$ 100.000,00 (cem mil reais) para atualização do Verificador de Conformidade e do Gerenciador de Políticas de Assinatura Digital, com validade até 01/03/2018. Apoiou iniciativas de digitalização de serviços de governo, como a Carteira Nacional de Habilitação Eletrônica (CNH-e) e o Sistema Online para Registro de Programas de Computador**,** além de celebrar acordo com o TSE para consulta de dados biométricos. O ITI apoiou a iniciativa do INPI em novo modelo de Registro de Software com uso exclusivo de certificação digital ICP - Brasil. O Instituto esteve presente nos principais eventos voltados à segurança da informação, desmaterialização de processos, defesa e iniciativas afins, tais como: a) etapa regional do *Security Leaders*, evento da área de Segurança Cibernética e Risco; b) V Seminário Nacional de certificação Digital, realizado em São Paulo nos dias 24 e 25/05/2017; c) *Encuentro de Transformación Digital*, realizado no Uruguai em 23/08/2017; d) *Biometrics HITech* e do XIV Congresso Brasileiro de Identificação, sobre biometria, realizado em 29/08/2017 em São Paulo; e e) Encontro de presidentes das empresas estaduais de TI organizado pela ABEP, realizado em Brasília no dia 24/11/2017. O ITI recebeu o "Troféu JK" como reconhecimento ao empreendedorismo na área da certificação digitital ICP – Brasil e das iniciativas em fomentar a criação de serviços digitais de governo, no dia 22/09/2017 em Brasília.

6. Promoção e Disseminação do Uso da Certificação Digital – ICP – Brasil: Sensibilização e Capacitação

Objetivo 6.1:	Apresentar a sociedade *cases* que demandam a tecnologia ICP – Brasil, sensibilizar gestores públicos e privados em relação ao tema e estimular a adoção de tecnologias mais sustentáveis e a eliminação do uso de insumos.
Ação:	Realizar o Fórum de Certificação Digital - CertForum
Meta	Realizar duas etapas do evento anualmente, sendo uma em Brasília - DF
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	ASCOM – Edmar da Silva Araújo
Resultados - 2017	A Assessoria de Comunicação do ITI foi responsável pela produção do site do evento 15º CertForum - Fórum de Certificação Digital que é o mais tradicional dos eventos realizados no país sobre a certificação digital ICP - Brasil, reunindo seletos público e palestrantes para a transmissão do conhecimento por meio de painéis e debates. O Fórum se realizará em duas etapas: Brasília-DF, nos dias 19,20 e 21 de setembro e em Recife, no mês de novembro. No período também foi realizada a quinta edição do Seminário Nacional de Certificação Digital, nos dias 24 e 25 de maio de 2017, em São Paulo, paralelamente à 22ª. *Cards Payment & Identification, maior feira de tecnologia para o setor de cartões, meios eletrônicos de pagamento, identificação e certificação digital da América Latina.* No evento foram abordados os seguintes temas: ICP - Brasil em números; Programa Crédito Digital, Medicina Digital: ICP - Brasil no sistema médico, Assinatura digital de documentos na BRF, o Sistema de Processo Eletrônico (e-TCESP) do Tribunal de Contas de São Paulo e Telemedicina: Prescrição eletrônica. Realizou duas etapas do 15° CertForum – Fórum de Certificação Digital. Na etapa nacional, em Brasília (19, 20 e 21 de setembro), o ministro-chefe da Casa Civil da Presidência da República Eliseu Padilha participou da solenidade de abertura. Elaborou novo site e marca. Publicou Plano de Dados Abertos. Sediou e transmitiu as reuniões do CG ICP - Brasil por meio de seu canal no *Youtube* (1000 inscritos).

Objetivo: 6.2:	Produzir material jornalístico, publicitário e de marketing que garanta a disseminação e o conhecimento da tecnologia ICP – Brasil, além de registrar eventos relevantes para a memória do ITI.
Ação:	Produção de boletim semanal, boletim interno, notas e *releases* à imprensa e atualização das mídias sociais com os devidos conteúdos produzidos pela ASCOM.
Meta	Manter os vários segmentos da sociedade informados sobre perspectivas mais aprofundadas dos temas sobre os benefícios e aplicações da Certificação Digital ICP–Brasil.
Prazo:	2017 e 2018 (Continuado)
Recursos Orçamentários	Ação orçamentária 2000 - Administração
Responsável:	ASCOM – Edmar da Silva Araújo
Resultados - 2017	A Assessoria de Comunicação – ASCOM, área responsável pela interlocução entre a Instituição e o cidadão, publicou 44 Boletins Digitais, totalizando 182 notícias distribuídas para 9.960 contatos. Divulgou suas ações nas redes sociais Facebook (4905 curtidas), Twitter (1148 seguidores) e Instagram (315 seguidores). Promoveu consulta pública sobre "Certificado Digital em Nuvem".

7. *Macroprocessos de Apoio e Reestruturação Organizacional*

Objetivo 7.1 :	Viabilizar a Implementação e Execução da Coleta Seletiva de Resíduos Recicláveis
Ação:	Tomar as providências necessárias à implementação da Coletiva Seletiva de Resíduos Recicláveis, de acordo com o Decreto n° 5.940, de 05/10/2066.
Meta:	Implantar a infraestrutura necessária e iniciar à Coletiva Seletiva de Resíduos Recicláveis – Unidade: 5 (percentual) de implantação.
Prazo:	2015 – 100% (2017)
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues
Resultados - 2017	Até o momento não foi possível implementar a coleta seletiva de resíduos.

Objetivo 7.2:	Gestão do Almoxarifado
Ação:	Desenvolver ações para o aperfeiçoamento da gestão do almoxarifado, de forma que seja possível manter e controlar o estoque físico e os correspondentes registros digitais, evitando-se também a aquisição de material via suprimento de fundos e dispensa de licitação.
Meta:	Manter e controlar o estoque do almoxarifado de acordo com as necessidades do Órgão – Unidade: inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação.
Prazo:	2017–Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação 2018-Inexistência de aquisição de material de consumo, via suprimento de fundos ou dispensa de licitação
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues
Resultados - 2017	De acordo com informação prestada pela Coordenação de Licitação e Contratos, houve Dispensa de Licitação para contratação de empresa para avaliar o imóvel, aquisição de bandeiras e pins, compra de tinta para manutenção de bens imóveis, manutenção de equipamentos de informática, aquisição de 4 aparelhos celulares e contratação de empresa para conserto de poltronas giratórias. As compras de material de consumo com suprimento de fundos atingiram o valor total de R$ 10.464,00.

Objetivo 7.3 :	Controle Patrimonial
Ação:	Aperfeiçoar o controle do acervo patrimonial do Instituto, de acordo com a legislação vigente, além de executar política de desfazimento regular de bens inservíveis, de modo a evitar a onerosidade com estoque e depósito dessa natureza de material.
Meta:	Eliminar as inconsistências e manter o sistema atualizado – Unidade: Zerar inconsistências e não manter estoque de bens inservíveis
Prazo:	2017 – Não apresentar inconsistências e não manter estoque de bens inservíveis 2018 – Não apresentar inconsistências e não manter estoque de bens inservíveis
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CLOG – Jorge Luís Rodrigues
Resultados - 2017	Foi designada uma Comissão para identificação dos bens inservíveis com vistas a seu desfazimento.

Objetivo 7.4:	Capacitação de Servidores Públicos Federais em Processo de Qualificação e Requalificação
Ação:	Promover a qualificação e requalificação de pessoal com vistas à melhoria continuada dos processos de trabalho, dos índices de satisfação pelos serviços prestados à sociedade e do crescimento profissional.
Meta:	Elaborar levantamento anual das necessidades de treinamento e participação em eventos e seminários, de forma otimizar a forma de contratação, evitando-se a dispensa de licitação. Unidade: Autorizar o treinamento ou participação em eventos e seminários, congressos e afins de, pelo menos, 20% do quadro de pessoal, passível de ser contemplado.
Prazo:	2017 – 20% 2018 – 20%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CGP – Roberto Bueno de Assunção
Resultados - 2017	Em face da restrição orçamentária imposta no primeiro semestre de 2017, somente 11 (onze) servidores e colaboradores tiveram treinamento nesse período. Os treinamentos realizados foram: 1) V ciclo de Reuniões Técnicas – Fiscalização de Contratos Terceirizados de mão de obra, ministrado pela Escola da AGU, com participação de 04 servidores – junho/2017. 2) SEI, SEI – Usar, SEI – Implantar e SEI – Administrar, com a participação de 7 (sete) pessoas entre servidores e colaboradores – abril, maio e junho/2017. No segundo semestre de 2017, foram realizados os seguintes treinamentos: 1) Curso "V Ciclo de Reuniões Técnicas – Fiscalização de Contratos de Terceirização de Mão de Obra", com participação de 02 servidores – julho/2017 2) Curso Gestão por Processos, com participação de 20 pessoas, dentre servidores e colaboradores – novembro/2017.

Objetivo 7.5:	Exame Periódico de Pessoal sem Vínculo
Ação:	Desenvolver ações necessárias à execução dos exames de saúde periódicos, em especial, para o pessoal sem vínculo empregatício.
Meta:	Viabilizar a realização de exames de saúde periódicos, em especial, para o pessoal sem vínculo empregatício. Unidade: fazer com que 100% do pessoal sem vínculo empregatício realize os exames de saúde periódico.
	2017 – 100% 2018 – 100%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CGP – Roberto Bueno de Assunção
Resultados - 2017	Informa-se que não foram realizados exames periódicos para servidores sem vínculos até a presente data, haja vista a dificuldade para contratação de empresa para um número tão limitado de servidores, pois atualmente o ITI dispõe de apenas 02 (dois) servidores sem vínculo.

Objetivo 7.6 :	Melhoria do Processo de Conformidade Contábil
Ação:	Identificação dos processos que necessitam de aprimoramento das ações, para que a conformidade seja realizada, de acordo com padrões de qualidade e segurança.
Meta:	Identificar os processos críticos e disponibilizar instruções e/ou capacitar os responsáveis pela conformidade contábil, de forma que sejam cumpridos os prazos com qualidade e eficiência. Unidade: Reduzir a zero as pendências e descumprimentos de prazo.
Prazo:	2017 – Reduzir a zero as pendências e descumprimentos de prazo. 2018 – Reduzir a zero as pendências e descumprimentos de prazo.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CCONT – Aiche Leite Mohd Saleh
Resultados - 2017	Procedidas as verificações processuais, da documentação pertinente aos pagamentos realizados, visando o registro da Conformidade de Registro de Gestão. Com isso, toda e qualquer pendência que possa acarretar restrições, foram solucionadas antes do período de fechamento do balancete mensal. Foi atendido o cumprimento dos prazos e a melhoria da qualidade do processo da conformidade tendo observadas as orientações nos instrumentos de análise, utilizando os mecanismos disponíveis no Manual do SIAFI – Macrofunções – com observância aos princípios da legalidade e anualidade. Assegurou-se a exatidão, confiabilidade, integridade e oportunidade nas informações contábeis, financeiras, administrativas e operacionais. Foram identificadas as inconsistências ou desequilíbrios nas Demonstrações Contábeis, mediante as transações CONDESAUD e CONAUD, e implementadas ações de forma que as mesmas fossem sanadas antes de fechamento mensal, do balancete contábil. Registradas conformidade contábil dos atos e fatos da gestão orçamentária, financeira e patrimonial, consistindo na certificação dos demonstrativos contábeis, gerados pelo Sistema Integrado de Administração Financeira do Governo Federal (SIAFI), e nas Conformidades de Registro de Gestão. As conformidades contábeis são mensais, e abrangendo os dois semestres, com exceção do mês de novembro, todos foram registrados **sem restrição.** Embora no mês de novembro tenha ocorrido restrição contábil,a mesma não comprometeu os atos e fatos administrativos praticados pelos gestores da Unidade. A restrição se deu por conta da ausência, da conformidade de registro de gestão, especificamente no dia 06/11/2017, por perda de prazo para registro, por parte do responsável pela conformidade, no SIAFI. Quanto ao Sistema de Concessão de Diárias e Passagens, foi administrado e gerenciado as aquisições de passagens realizadas pelas áreas demandantes, com observância dos procedimentos e prazos legais. Foi procedido o cadastramento, bem como a desabilitação de usuários, conforme demanda das Unidades, a nível de atuação e autoridade para operacionalização no SCDP.

Objetivo 7.7:	Implantar Novo Procedimento para Pagamento de Faturas
Ação:	Implantar novo procedimento para pagamento de faturas, de forma que os processos de pagamento sejam apartados do processo principal.
Meta:	Identificar os processos críticos e disponibilizar instruções e/ou capacitar os responsáveis pela conformidade contábil, de forma que sejam cumpridos os prazos com qualidade e eficiência. Unidade: Implantar o novo procedimento e estabelecer ponto de controle para apurar se a nova sistemática efetivamente permitiu agilizar o processo de pagamento.
Prazo:	2015 – 100 % implantado e controlado
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CPL – Nathércia Maria Ribeiro de A.C. Meleiro

Resultados - 2017	Procedimento implantado com sucesso. Internamente, a Portaria nº 74/2014, de lavra da CGPOA, conferiu agilidade e eficiência ao novo procedimento para pagamento de faturas, de modo que os atos de ordenação de despesa devem constar prévio e formalmente consignados em autos próprios ante aos autos de liquidação e pagamento. Registre-se, entretanto, que alterações nos procedimentos estão em estudo, em especial as relativas à folha de pagamento, de forma a evitar refazimentos, inconsistências e erros, além de imprimir maior controle e agilização do processo. O novo procedimento será objeto de mapeamento no segundo semestre de 2017.

Objetivo 7.8:	Melhoria do Processo de Fiscalização de Contratos
Ação:	Implementar melhoria nos processos de fiscalização de contratos, de forma que sejam revistas e padronizadas as planilhas de controle, que devem contemplar todos os itens a serem observados, com o objetivo de minimizar eventuais riscos. Adotar outros procedimentos, que permitam a melhoria de processo, tais como: treinamentos, cartilhas, estágios, etc..
Meta:	Dispor de material de apoio padronizado e automatizado, que reduzam os riscos de eventuais erros. Unidade: 100% das planilhas revisadas e 100% funcionários envolvidos treinados.
Prazo:	2017 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados. 2018 – 100% das planilhas revisadas e 100% funcionários envolvidos treinados.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade.
Responsável	CGPOA/CFC – José Adalberto Ribeiro de Andrade
Resultados - 2017	As planilhas de controle foram revisadas e padronizadas, dentro do prazo estabelecido (até dez/2015).

Objetivo 7.9:	Solução para Manutenção Predial
Ação:	Buscar solução para Manutenção Predial com a melhor relação custo-benefício.
Meta:	Dispor de serviços necessários à Manutenção predial, com atendimento tempestivo, de forma que sejam minimizados os riscos inerentes. Unidade: Implantar 100% da solução.
Prazo:	2017 – Implantar 100% da solução. 2018 – Implantar 100% da solução.
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade.
Responsável	CGPOA/CFC - José Adalberto Ribeiro de Andrade
Resultados - 2017	Encontra-se em análise novas possibilidades de contratação desses serviços (*facilities*) que imprimam maior qualidade e menor preço.

Objetivo 7.10:	Gerenciamento da infraestrutura tecnológica institucional
Ação:	Manter a infraestrutura de hardware atualizada e operacional para garantir o apoio tecnológico contínuo às aplicações do negócio.
Meta:	**Parque computacional crítico em produção atualizado e em garantia:** Indicador: % (percentual) do parque crítico em garantia. Métrica: 95% **Adequação e evolução da infraestrutura de armazenamento, conectividade e do parque de ativos às necessidades do ITI:** Indicador: % (percentual) de conformidade às necessidades do Instituto. Métrica: 95% de conformidade aos objetivos de negócio
Prazo:	2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 – Administração
Responsável	CGPOA/CODIS

Resultados - 2017

1º Semestre de 2017
Adequação e evolução da infraestrutura (2017) – 95%

Levantamento realizado – Julho/2017

Equipamento	Quantidade total	Quantidade em garantia	Percentual em garantia
Switches	31	6	19.35%
Servidores	30	0	0.00%
Balanceador	2	0	0.00%
Storage	2	1	50.00%
Controladora sem fio	1	0	0.00%
Access Points	13	0	0.00%
Desktops – dell 780	18	0	0.00%
Desktops – dell 790	65	0	0.00%
Desktops – Itautec	83	0	0.00%
Notebooks – HP	2	0	0.00%
Notebooks – TCORP	23	0	0.00%
Impressoras	33	8	24.24%
Câmeras – CFTV	13	0	0.00%
Videoconferência – RSS	1	0	0.00%
VIdeoconferência – Gatekeeper	1	0	0.00%
Videoconferência – HDX	2	0	0.00%
Fitoteca	2	0	0.00%
TOTAL	**322**	**15**	**4.66%**

Apesar da grande maioria do parque de equipamentos do ITI estarem fora de garantia, eles ainda atendem às necessidades de negócio.
Desde 2015 até o presente momento não foi possível fazer novos investimentos na renovação do parque do ITI administrado pela CODIS, em razão de contingenciamentos que vem acontecendo periodicamente.

2º Semestre de 2017
Em 2017 foi realizada contratação para renovação de 100% do parque de estações de trabalhos e notebooks no Instituto, bem como servidores. O contrato encontra-se em vigor sendo a previsão de conclusão da substituição dos equipamentos é março de 2018.

Objetivo 7.11:	Disponibilizar e Gerenciar softwares aplicativos em alinhamento com os requisitos do negócio
Ação:	Traduzir os requisitos de negócio em especificações de projeto para a aquisição, a manutenção e o desenvolvimento de softwares do Instituto, a fim de apoiar de forma adequada as operações do negócio, levando em consideração o direcionamento tecnológico e a arquitetura de informação.
Meta:	**Contratação de fábrica de software para manutenção e desenvolvimento de sistemas** Indicador: % (percentual) softwares desenvolvidos/mantidos Métrica: 80% de contratações de fábrica de software para manter/desenvolver os softwares priorizados pelo CETI **Manutenção dos sites do ITI** Indicador: Quantidade de sites mantidos **Aquisição de softwares aplicativos para alcançar os objetivos do negócio:** Indicador: % (percentual) de softwares aplicativos do Órgão gerenciados tecnicamente pela CGPOA/CODIS. Métrica: 60% dos softwares gerenciados pela CGPOA/CODIS
Prazo:	2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 – Administração
Responsável	CGPOA/CODIS

Resultados – 2017	**1º Semestre de 2017** - Contratação de fábrica de software para manutenção e desenvolvimento de sistemas (2015) – 100% - Manutenção dos sites do ITI* – 5 sites mantidos (Portal ITI; Portal CODIS; Portal Intranet; Sistemas Web Auditoria; e Sistemas Web Antifraude Teste e Homologação) - Aquisição e desenvolvimento de softwares aplicativos para alcançar os objetivos do negócio** – 100% *Portais alinhados com os requisitos do negócio **Alteração da Meta de: **Aquisição de softwares aplicativos para alcançar os objetivos do negócio** para **Aquisição e desenvolvimento de softwares aplicativos para alcançar os objetivos do negócio.** Não ocorreram aquisições de softwares, porém foram desenvolvidos ou aperfeiçoados internamente. **2º Semestre de 2017** 100% dos softwares priorizados pelo CETI encontram-se no escopo da contratação da Fábrica de Software. Também foi realizada contratação de uma Aplicação Analítica Para Tomada de Decisão visando atender demandadas das áreas finalísticas da DAFN.

Objetivo 7.12:	Gerenciamento da Governança de TI no âmbito da CODIS
Ação:	Analisar as tecnologias existentes e planejar qual direcionamento é apropriado para implementar a estratégia de TI e identificar quais tecnologias geram oportunidades de negócio, com a finalidade de gerar valor para o negócio e aderência a requisitos e *compliance*.
Meta:	**Adoção de um Modelo de controle para a Governança de TI:** Indicador: Quantidade de processos da CGPOA/CODIS aderentes ao COBIT. Métrica: 3 (três) objetivos de controle de Governança aderentes ao COBIT por ano. **Aplicação de um Modelo de Gerenciamento de Projetos:** Indicador: % (percentual) de projetos da CGPOA/CODIS que seguem os padrões e as práticas de gerenciamento de projetos. Métrica: 90% dos projetos da CGPOA/CODIS aderentes às boas práticas de gerenciamento de projetos. **Adoção de um modelo de melhores práticas para Gerenciamento de Serviços de TI:** Indicador: % (percentual) de serviços de TI ofertados pela CGPOA/CODIS que seguem as melhores práticas de gerenciamento de serviços. Métrica: 25% dos serviços aderentes às boas práticas de gerenciamento de projetos **Contratação de Serviços em alinhamento as necessidades organizacionais:** Indicador: Quantidade de serviços contratados. Métrica: Mínimo dois serviços contratados ou mantidos por ano.
Prazo:	2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 – Administração
Responsável	CGPOA/CODIS
Resultados - 2017	**1º Semestre de 2017** **Adoção de um Modelo de controle para a Governança de TI (2015) –** 3 (três) objetivos: 1. Monitorar e Avaliar – Monitorar e Avaliar Desempenho (ME1 - Monitoramento de Ativos de Rede) 2. Entregar e Suportar – Gerenciar Capacidade e Desempenho (DS3 - Gerenciamento de armazenamento dos compartilhamentos e caixas de e-mail; Desempenho de serviços de mensagens e de sistemas) 3. Adquirir e Implementar – Identificar Soluções Automatizadas (AI1- Automatização de sistemas de monitoramento e de gestão de usuários) **Aplicação de um Modelo de Gerenciamento de Projetos** – foi atingida a meta de 90%, considerando o resultado dos seguintes projetos: 1. Sistema Antifraudes – 85% Aderente; 2. Sistemas da Diretoria de Auditoria, Fiscalização e Normalização – 90% Aderente 3. Melhoria da Infraestrutura de Serviços da Intranet – 95% Aderente; **Adoção de um modelo de melhores práticas para Gerenciamento de Serviços de TI** – realizado 35%. Aplicado o Gerenciamento em Serviços de TI em: 17. Atendimento ao usuário; 18. Gestão de serviços e redes; 19. Gestão de Contratos e licitações de TI; 20. Gestão de serviços de desenvolvimento, fábrica de software e contagem de pontos de função. **Contratação de Serviços em alinhamento as necessidades organizacionais** – 4 (quatro) serviços contratados, a saber: 12. Fábrica de Software - Desenvolvimento 13. Contagem e validação de contagem de Pontos de Função; 14. Suporte e atendimento aos usuários; 15. Administração de redes e serviços de redes de dados. **2º Semestre de 2017** **Adoção de um Modelo de controle para a Governança de TI (2015) – 3 (três) objetivos:** 1. Monitorar e Avaliar – Monitorar e Avaliar Desempenho (ME1 - Monitoramento de Ativos de Rede)

	2. Entregar e Suportar – Gerenciar Capacidade e Desempenho (DS3 - Gerenciamento de armazenamento dos compartilhamentos e caixas de e-mail; Desempenho de serviços de mensagens e de sistemas) 3. Adquirir e Implementar – Identificar Soluções Automatizadas (AI1- Automatização de sistemas de monitoramento e de gestão de usuários) **Aplicação de um Modelo de Gerenciamento de Projetos – foi atingida a meta de 90%, considerando o resultado dos seguintes projetos:** 1. Sistema Antifraudes – 85% Aderente; 2. Sistemas da Diretoria de Auditoria, Fiscalização e Normalização – 90% Aderente 3. Melhoria da Infraestrutura de Serviços da Intranet – 95% Aderente; **Adoção de um modelo de melhores práticas para Gerenciamento de Serviços de TI – realizado 50%. Aplicado o Gerenciamento em Serviços de TI em:** 1. Atendimento ao usuário; 2. Gestão de serviços e redes; 3. Gestão de Contratos e licitações de TI; 4. Gestão de serviços de desenvolvimento, fábrica de software e contagem de pontos de função. **Contratação de Serviços em alinhamento as necessidades organizacionais – 5 (cinco) serviços contratados, a saber:** 1. Fábrica de Software - Desenvolvimento 2. Contagem e validação de contagem de Pontos de Função; 3. Suporte e atendimento aos usuários; 4. Administração de redes e serviços de redes de dados; 5. Segurança como serviço (camada de segurança para acesso à INFOVIA).

Objetivo 7.13:	Gerenciamento da segurança dos ambientes físico e lógico da CODIS
Ação:	Manter os ativos e processos internos aderentes à legislação de segurança vigente.
Meta:	**Alinhamento com Política de Segurança da Informação e Comunicações (POSIC) e às Normas Complementares do Gabinete de Segurança Institucional (NC/GSI):** Indicador: Quantidade de ações/rotinas aderentes à POSIC e às NC/GSI. Métrica: 25 ações/rotinas aderentes à POSIC e às NC/GSI **Garantir a disponibilidade dos ativos críticos gerenciados** Indicador: Tempo de indisponibilidade devido a incidentes no ambiente físico e lógico Métrica: Tempo de indisponibilidade dos ativos críticos < 0,5 % **Garantir a confidencialidade, autenticidade, integridade e controle de acesso das informações críticas** Indicador: Quantidade de incidentes causados por falhas ou violação da segurança Métrica: Incidentes causados por falhas ou violação da segurança < 5 por ano
Prazo:	2017 a 2018 (continuada)
Recursos Orçamentários:	Ação orçamentária 2000 – Administração
Responsável	CGPOA/CODIS
Resultados - 2017	Meta alcançada: Incidentes causados por falhas ou violação da segurança < 5 por ano: Não houve Incidentes causados por falhas ou violação de segurança até a presente data (23/01/2018).

Objetivo 7.14:	Promover estudos e submeter à aprovação das Autoridades Competentes proposta de reestruturação organizacional do ITI, adequada às suas responsabilidades institucionais
Ação:	Acompanhar aprovação junto ao MPOG do processo de carreira do ITI. Encaminhar proposta consolidada do regimento interno para aprovação.
Meta:	Aprovação de concurso para quadro próprio. Contratação de aprovados no concurso.
Prazo:	2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA

Resultados - 2017	Foi encaminhada proposta de Regimento Interno para aprovação da Casa Civil, através do ofício n° 048/2015-GAB/ITI-PR, de 02 de outubro de 2015, objeto do Processo n° 00100.000197/2013-81, pendente de publicação até a presente data. Com o advento da Medida Provisória n° 726, de 12 de maio de 2016, o ITI passou a ser vinculado ao Ministério da Ciência, Tecnologia, Inovações e Comunicações, fato que somente foi revertido em 10 de outubro de 2016, com a publicação do Decreto n° 8.872. Por outro lado, o Decreto 8.985, de 8 de fevereiro de 2017, estabeleceu nova estrutura regimental do ITI e prazo de até 02.05.2017 para publicação do Regimento Interno. Com a posse dos novos dirigentes, a partir de 28.04.2017, a estrutura das áreas encontra-se sob análise, de forma que o regimento interno somente será aprovado, uma vez definida a nova composição organizacional do Instituto. O pleito para adoção do Plano de Carreira de C&T no âmbito do Instituto foi encaminhado para o Ministério do Planejamento, Desenvolvimento e Gestão - MPDG, em 19.11.2013, acompanhado de Parecer favorável a seu atendimento. A matéria permanece sob os cuidados do MPDG, sem avanços até a presente data. Com a posse dos novos dirigentes, foi desenvolvido entendimento com a Infraero para cessão de funcionários ao Instituto. A seleção encontra-se em curso e a intenção é alocar, pelo menos um funcionário, nas áreas onde não haja substituto.

Objetivo 7.15:	Implementar gestão com vistas a aquisição de sede própria e/ou melhoramento nas instalações atuais.
Ação:	Criar GT para propor alternativas para a sede própria.
Meta:	Dispor de sede própria ou melhorias nas instalações atuais.
Prazo:	2017 a 2018
Recursos Orçamentários:	Ação orçamentária 2000 - Administração
Responsável	CGPOA -
Resultados - 2017	No dia 28.04.2017, foi alterada a cúpula do Instituto e nomeados novo Diretor-Presidente e dois novos Diretores. A nova Administração empreendeu esforços no sentido de buscar um novo espaço para a sede do Instituto, no entanto, o prazo para renovação do contrato de aluguel vigente era muito exíguo. Dessa forma, optou-se por renegociar o valor do aluguel para o período de mais um ano. O valor foi reduzido significativamente, considerando-se as condições favoráveis do mercado. De toda forma, estão sendo envidados esforços no sentido de buscar um novo espaço compatível com a necessidade do Instituto, que atenda às exigências de segurança física e, de preferência, sem obrigações pecuniárias.

8. Reestruturação Orçamentária

Objetivo 8.1:	Melhoria da Gestão de Orçamento e Execução Financeira
Ação:	Aperfeiçoamento da Gestão Conjunta do Orçamento e da Execução Financeira do Instituto, com vistas à otimização do relacionamento com Setorial.
Meta:	Maximização do uso dos recursos orçamentários – Unidade: percentual de utilização dos recursos
Prazo:	2017 – 95% 2018 – 95%
Recursos Orçamentários:	Ação orçamentária 2000 – Administração da Unidade
Responsável:	CGPOA/CPO e CGPOA/COF – Maria Izilda Ferreira e Joseni A. Belmiro de A. Silva
Resultados - 2017	O exercício de 2017 foi marcado por forte contingenciamento orçamentário no primeiro semestre de 2017. No entanto, a partir do segundo semestre, a Casa Civil da Presidência da República, sensibilizada com a importância da Certificação Digital para a economia nacional, descontingenciou todo o crédito orçamentário. Desta feita, foi possível renovar parte do parque tecnológico que estava fora de garantia, além de contratar a manutenção de equipamentos essenciais ao funcionamento do Sistema Nacional de Certificação Digital. O ITI finalizou o exercício de 2017 com uma dotação de crédito da ordem de R$ 14.988.000,00 e empenhou R$ 14.828.247,00, ou seja, executou aproximadamente 98,93% do orçamento.

9. Monitoramento de Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP Brasil.

Objetivo 9.1:	Monitorar Projetos de Lei que disciplinem o uso de assinaturas eletrônicas e a prestação de serviços de certificação digital de interesse da ICP - Brasil.
Ação:	Conhecer, acompanhar, prestar apoio técnico para que os Projetos de Lei que envolvam assinaturas eletrônicas e a prestação de serviços de certificação digital contribuam para a massificação do uso da certificação digital da ICP - Brasil.
Meta	Contribuir para a Massificação da Certificação Digital ICP Brasil.
Prazo:	2017 e 2018 (continuado)
Recursos Orçamentários	Ação orçamentária 2000 – Administração da Unidade
Responsável:	Gabinete
Resultados - 2017	O ITI monitorou a publicação das leis que disciplinam o uso de assinaturas digitais produzidas pelo certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e publicou em seu

	sítio - www.iti.gov.br - notícias sobre esses textos legais. - Decreto nº 8.985, que aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das funções de confiança do Instituto Nacional de Tecnologia da Informação – ITI; - http://antigo.iti.gov.br/noticias/indice-de-noticias/5264-decreto-sobre-estrutura-regimental-do-iti-e-publicado-no-diario-oficial-da-uniao - acordo firmado entre os países do Mercosul e o Chile para validar o uso de documentos digitais, no comércio entre as nações - http://antigo.iti.gov.br/noticias/indice-de-noticias/5263-presidente-assina-acordo-para-uso-do-certificado-de-origem-digital-no-mercosul - ECDs, livros contábeis emitidos em formato eletrônico, devem ser assinadas, independentemente de outras assinaturas, por um certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil de pessoa jurídica - http://antigo.iti.gov.br/noticias/indice-de-noticias/5312-certificado-icp-brasil-de-pessoa-juridica-torna-se-obrigatorio-para-assinatura-da-ecd - Tribunais do Distrito Federal e de Minas Gerais adotam nova versão do Pje - http://antigo.iti.gov.br/noticias/indice-de-noticias/5306-tribunais-do-distrito-federal-e-de-minas-gerais-adotam-nova-versao-do-pje - Empresário com quatro empregados? Você vai precisar de um certificado ICP-Brasil - http://antigo.iti.gov.br/noticias/indice-de-noticias/5303-empresario-com-quatro-empregados-voce-vai-precisar-de-um-certificado-icp-brasil - Tribunal Regional Federal da 3ª Região torna obrigatório uso do processo digital - http://antigo.iti.gov.br/noticias/indice-de-noticias/5297-tribunal-regional-federal-da-3-regiao-torna-obrigatorio-uso-do-processo-digital - ICP-BRASIL recebe selo de conformidade WebTrust CA - http://antigo.iti.gov.br/noticias/indice-de-noticias/5294-icp-brasil-recebe-selo-de-conformidade-webtrust-ca1 - Certificado digital deve ser usado por contribuintes no acesso a serviços restritos na SEFAZ-PI - http://antigo.iti.gov.br/noticias/indice-de-noticias/5336-certificado-digital-deve-ser-usado-por-contribuintes-no-acesso-a-servicos-restritos-na-sefaz-pi-1 - Presidente da República empossa nova diretoria do ITI - http://antigo.iti.gov.br/noticias/indice-de-noticias/5322-presidente-da-republica-empossa-nova-diretoria-do-iti1 - Senai Ceará adota diploma digital assinado com certificado ICP-Brasil - http://antigo.iti.gov.br/noticias/indice-de-noticias/5319-senai-ceara-adota-diploma-digital-assinado-com-certificado-icp-brasil - Certificado ICP-Brasil é obrigatório para acesso aos plantões on-line do Tribunal de Justiça de Goiás - http://antigo.iti.gov.br/noticias/indice-de-noticias/5318-certificado-icp-brasil-e-obrigatorio-para-acesso-aos-plantoes-on-line-do-tribunal-de-justica-de-goias

REPÚBLICA FEDERATIVA DO BRASIL

Presidente

Michel Miguel Elias Temer Lulia

Casa Civil da Presidência da República

Ministro-Chefe da Casa Civil

Eliseu Lemos Padilha

Instituto Nacional de Tecnologia da Informação – ITI

Autarquia vinculada à Casa Civil da Presidência da República

Diretor – Presidente

Gastão José de Oliveira Ramos

Diretor de Infraestrutura de Chaves Públicas – DINFRA

Waldeck Pinto de Araújo Júnior

Diretor de Auditoria, Fiscalização e Normalização – DAFN

Rafaelo Abritta

Coordenador Geral de Planejamento, Orçamento e Administração

Ronoilton Gonçalves

Procurador Chefe

Alexandre Munia Machado

Planejamento Estratégico 2015-2018

Desenvolvido pelo Grupo Técnico de Trabalho, designado pela Portaria n° 24, de 17 de outubro de 2014, cujos integrantes são:

Alessandra Maria Costa e Lima – CODIS/CGPOA
Alexandre Menezes Ribeiro - DAFN
José Rodrigues Gonçalves Júnior – DINFRA
Maria Izilda Ferreira – CPO/CGPOA
Ruy César Ramos Filho – GABINETE

Brasília – Fevereiro/2018

ANEXO 3

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO – PDTIC 2017 - 2018

PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Instituto Nacional de Tecnologia da Informação – ITI

ITI
Instituto Nacional de
Tecnologia da Informação

Plano Diretor de Tecnologia da Informação e Comunicação

2017-2018

Equipe de Elaboração do PDTIC

André Quezado

Antônio de Souza Ferreira

Geraldo Clay de Sousa Maciel

Ronald Luiz Silva Siqueira

Ruy César Ramos Filho

Responsável pela Aprovação do PDTIC

Gastão José de Oliveira Ramos – Diretor-Presidente

Comitê de TI (CETI)

Coordenador: Ruy César Ramos Filho

Secretária: Maria Izilda Ferreira

Representantes das áreas

Gabinete - Adriana Fetter Dias da Costa e Ruy César Ramos Filho

Procuradoria - André Pinto Garcia e Danielle Salviano Barbosa

DAFN - Pedro Pinheiro Cardoso e Wilson Roberto Hirata

DINFRA - José Rodrigues Gonçalves Júnior, André Machado Caricatti, Anderson S. Araújo

CGPOA – Ronoilton Gonçalves

Sumário

VISÃO GERAL

Apresentação

O Plano Diretor de Tecnologia da Informação e Comunicações – PDTIC – é um instrumento de diagnóstico, planejamento e gestão de recursos e processos de Tecnologia da Informação e Comunicação (TIC). Tem como objetivo determinar as prioridades de investimento e alocação de recursos nos diversos projetos e ações de TIC no Instituto Nacional de Tecnologia da Informação (ITI). Permite o alinhamento entre as atividades de TIC e o negócio da organização, a otimização dos recursos disponíveis, o acompanhamento do estágio de desenvolvimento dos projetos, solução de conflitos relativos a recursos e monitoramento dos níveis de serviço de TIC e suas melhorias.

O presente PDTIC tem como objetivo sistematizar o planejamento da gestão de TIC para o período de 2017 e 2018.

A revisão do documento deverá ser anual e a revisão das prioridades deverá ser periódica, em consonância com as reuniões do Comitê Estratégico de Tecnologia da Informação - CETI.

Os procedimentos para elaboração foram definidos de acordo com o Planejamento Estratégico do ITI e também o levantamento de necessidades das seguintes áreas:

- Gabinete
- Diretoria de Infraestrutura de Chaves Públicas - DINFRA
- Diretoria de Auditoria, Fiscalização e Normalização DAFN
- Coordenação-Geral de Planejamento, Orçamento e Administração - CGPOA

Introdução

O planejamento é uma obrigação legal, estipulado no artigo 174 da Constituição Federal de 1988:

> Art. 174. Como agente normativo e regulador da atividade econômica, o Estado exercerá, na forma da lei, as funções de fiscalização, incentivo e planejamento, sendo este determinante para o setor público e indicativo para o setor privado.

O Decreto-lei 200 de 1967 estabelece o planejamento como um princípio fundamental da Administração Pública Federal:

> Art. 6º. As atividades da Administração Pública Federal obedecerão aos seguintes princípios fundamentais:
> I – Planejamento
> II – Coordenação
> III – Descentralização
> IV – Delegação de Competência
> V - Controle

O modelo de governança *Control Objectives for Information and Related Technology* (Cobit) estabelece, no processo PO1, Definir um Plano Estratégico de TI:

> O planejamento estratégico de TI é necessário para gerenciar todos os recursos de TI em alinhamento com as prioridades e estratégias de negócio. A função de TI e as partes interessadas pelo negócio são responsáveis por garantir a otimização do valor a ser obtido do portfólio de projetos e serviços. O plano estratégico deve melhorar o entendimento das partes interessadas no que diz respeito a oportunidades e limitações da TI, avaliar o desempenho atual e esclarecer o nível de investimento requerido. A estratégia e as prioridades de negócio devem ser refletidas nos portfólios e executadas por meio de planos táticos de TI que estabeleçam os objetivos concisos, tarefas e planos bem definidos e aceitos por ambos, negócio e TI.

A Instrução Normativa SLTI/MP nº 04/2014 estabelece no artigo 4º:

> As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, elaborado em harmonia com o PDTIC, alinhado ao planejamento

estratégico do órgão ou entidade.

O art. 1º do ANEXO I do Decreto nº 8.985, de 8 de fevereiro de 2017 afirma que::

Art. 1º O Instituto Nacional de Tecnologia da Informação - ITI, autarquia federal criada pelo art. 12 da Medida Provisória no 2.200-2, de 24 de agosto de 2001, com sede e foro no Distrito Federal, vinculada à Casa Civil da Presidência da República, com a finalidade de ser a Autoridade Certificadora Raiz - AC Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, tem as seguintes competências:

I - executar as políticas de certificação e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

II - propor a revisão e a atualização das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil;

III - gerenciar os certificados das Autoridades Certificadoras - AC de nível imediatamente subsequente ao seu, incluindo emissão, expedição, distribuição e revogação desses certificados;

IV - gerenciar a lista de certificados emitidos, revogados e vencidos;

V - executar as atividades de fiscalização e de auditoria das AC, das Autoridades de Registro - AR e dos prestadores de serviços habilitados na ICP-Brasil, em conformidade com as diretrizes e as normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil;

VI - aplicar sanções e penalidades, na forma da lei; e

VII - credenciar as AC, as AR e os prestadores de serviço de suporte da ICP-Brasil.

Parágrafo único. Compete, ainda, ao ITI:

I - promover o relacionamento com instituições congêneres no País e no exterior;

II - celebrar e acompanhar a execução de convênios e de acordos internacionais de cooperação, no campo das atividades de infraestrutura de chaves públicas e áreas afins, ouvido o Comitê Gestor da ICP-Brasil;

III - estimular a participação de universidades, de instituições de ensino e da iniciativa privada em pesquisa e desenvolvimento, nas atividades de interesse da área da segurança da informação e da infraestrutura de chaves públicas;

IV - estimular e articular projetos de pesquisa científica e de desenvolvimento

> tecnológico voltados à ampliação da cidadania digital, por meio da utilização de certificação e assinatura digitais ou de outras tecnologias que garantam a privacidade, a autenticidade e a integridade de informações eletrônicas;
>
> V - executar outras atribuições que lhe forem cometidas pelo Comitê Gestor da ICP-Brasil; e
>
> VI- fomentar o uso de certificado digital através de dispositivos móveis para toda a administração pública federal.

O Planejamento Estratégico será refletido no planejamento das ações da TIC. Dessa forma será possível apoiar o ITI no alcance da missão de "atuar na inovação, regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente."

Termos e Abreviações

Termo	Descrição
BSC	*Balanced Scorecard* – metodologia de gestão de desempenho desenvolvida por Robert Kaplan e David Norton
CETI	Comitê Estratégico de Tecnologia da Informação
COBIT	*Control Objectives for Information and Related Technology* – guia de boas práticas direcionado para a gestão de Tecnologia da Informação
EqPDTIC	Equipe de Elaboração do PDTIC
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
ITIL	*Information Technology Infrastructure Library* – conjunto de boas práticas aplicadas na infraestrutura, operação e manutenção de serviços de TI
PMBoK	*Project Management Body of Knowledge* – conjunto de boas práticas para gerenciamento de projetos
PPA	Plano Plurianual
PDTIC	Plano Diretor de Tecnologia da Informação
SLTI	Secretaria de Logística e Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

Metodologia Aplicada

Para a elaboração do PDTIC foram utilizados o Planejamento Estratégico do Instituto Nacional de Tecnologia da Informação, o levantamento de necessidades consolidados das áreas, o Modelo de Referência do PDTIC do SISP, a EGTI 2013-2015 e o Guia de Elaboração de PDTIC do SISP.

Como a atividade-fim do ITI é a Tecnologia da Informação, no seu Planejamento Estratégico já são apresentados, a nível macro, as necessidades tecnológicas e de informação. Sendo assim, o PDTIC 2017-2018 apresenta-se como um planejamento tático, apresentando as prioridades estabelecidas pelo CETI com base no Planejamento Estratégico do ITI.

Documentos de Referência

Na elaboração deste PDTIC foram considerados os seguintes documentos:

Documento de Referência	Descrição
Constituição da República Federativa do Brasil de 1988	Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência.
Decreto-lei nº 200, de 25 de fevereiro de 1967	Art. 6º As atividades da Administração Federal obedecerão aos seguintes princípios fundamentais: Planejamento, Coordenação, Descentralização, Delegação de Competência e Controle.
Decreto nº 7.579/2011	Art. 1º Ficam organizados sob a forma de sistema, com a denominação de Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, o planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de tecnologia da informação dos órgãos e entidades da administração pública federal direta, autárquica e fundacional, em articulação com os demais sistemas utilizados direta ou indiretamente na gestão da informação pública federal.
Plano Plurianual – PPA	**Objetivo:** 0605 - Ampliar a oferta de serviços públicos de excelência ao cidadão, às empresas e às demais organizações da sociedade, mediante a melhoria dos marcos legais, dos processos de trabalho e da tecnologia da informação. **Órgão Responsável:** Ministério do Planejamento, Orçamento e Gestão **Iniciativa:** 02D2 - Massificação e aperfeiçoamento da Certificação Digital

	ICP Brasil e outras tecnologias de segurança da informação e identificação digital necessárias às transações eletrônicas de interesse da União, dos Estados, dos Municípios e da sociedade, mediante a garantia de pleno funcionamento da Infraestrutura de Chaves Públicas Brasileira e de Carimbo do Tempo da ICP Brasil, como forma de assegurar sua interoperabilidade, capilaridade, acessibilidade e eficácia jurídica às transações e documentos eletrônicos, bem como contribuir para a preservação do meio ambiente ao permitir a desmaterialização de processos e documentos
Medida Provisória Nº 2.200/2001	Deu início à implantação do sistema nacional de certificação digital da ICP-Brasil
Decreto nº 7.174/2010	Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal.
Decreto nº 4.689/2003	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências.
Instrução Normativa SLTI/MP nº 04 de 11 de setembro de 2014	Art. 2º, inciso XXVII - Plano Diretor de Tecnologia da Informação (PDTI): instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período. Art. 4º As contratações de que trata esta IN deverão ser precedidas de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação - PDTI.
Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
PDTIC ITI 2015-2016	Plano Diretor de TI do ITI – 2015-2016
Planejamento Estratégico 2015-2018 ITI	Planejamento Estratégico desenvolvido pelo Grupo Técnico de Trabalho designado na Portaria n° 9, de 07 de março de 2014, com a colaboração de todas as áreas do Instituto. Disponível em http://www.iti.gov.br/institucional/politicas2
Manual de apoio à Elaboração do Planejamento Estratégico e ao Levantamento de Necessidades Consolidado	Manual elaborado pela equipe da CODIS contendo orientações sobre o Inventário de Necessidades.
Padrões de Interoperabilidade de Governo Eletrônico (e-ping)	Disponível em http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade
Modelo de Acessibilidade do Governo Eletrônico (e-mag)	Disponível em http://www.governoeletronico.gov.br/acoes-e-projetos/e-MAG
Cobit 4.1	PO1 – Definir um Plano Estratégico de TI PO1.2 – Alinhamento entre TI e Negócio PO1.4 – Plano Estratégico de TI

Processo de Elaboração de PDTIC e Modelo de Referência de PDTIC 2011-2012	Metodologia proposta pelo SISP, a qual dispõe sobre os padrões, orientações, diretrizes e *templates* para elaboração do Plano Diretor de Tecnologia da Informação.
Guia de Elaboração de PDTIC do SISP	Disponível em http://www.governoeletronico.gov.br/biblioteca/arquivos/guia-de-elaboracao-de-PDTIC-do-sisp-versao-1.0/view?searchterm=guia%20de%20elabora%C3%A7%C3%A3o%20PDTIC
Acórdão 2.585/2012-TCU-Plenário	Levantamento do Perfil da Governança de TI na Administração Pública Federal 2012
Acórdão 2.308/2010-TCU-Plenário	Levantamento do Perfil da Governança de TI na Administração Pública Federal 2010
Acórdão 1.603/2008-P do TCU	Situação da Governança de Tecnologia da Informação – TI na Administração Pública Federal. Ausência de Planejamento Estratégico Institucional, deficiência na estrutura de pessoal, tratamento inadequado à confidencialidade, integridade e disponibilidade das informações

Princípios e Diretrizes

Os Princípios deste PDTIC serão:

Princípio	Fonte
Alinhamento dos objetivos institucionais de TIC às estratégias de negócio e aperfeiçoar a governança de TI.	COBIT 4.1 Acórdão 1.603/2008 TCU-PLENÁRIO
As contratações de bens e serviços de TIC deverão ser precedidas de planejamento, seguindo o previsto no PDTIC.	IN SLTI/MP Nº 04 Acórdão 1.603/2008 Plenário TCU Acórdão 1.558/2003 TCU-PLENÁRIO
Planejamento dos investimentos de hardware e software seguindo políticas, diretrizes e especificações definidas em instrumentos legais.	IN SLTI/MP Nº 04
Estímulo à atuação dos servidores do ITI como gestores, terceirizando a execução das atividades que não integrem as atribuições finalísticas do Órgão.	Art. 37, inciso II, Constituição Federal de 1988 Decreto-Lei Nº 200/1967 Decreto Nº 2.271/1997 Acórdão 341/2009 TCU-PLENÁRIO
Estímulo ao desenvolvimento, à padronização, à integração, à interoperabilidade, à normalização dos serviços de produção e disseminação de informações, de forma desconcentrada e descentralizada.	Decreto 7.579/2011
Garantia da segurança da Informação e Comunicações.	IN GSI/PR Nº 01

As Diretrizes serão:

Diretrizes
Promover a governança de TIC no Órgão.
Buscar excelência, inovação e criatividade na gestão.
Investir no aumento da produtividade e otimização dos recursos de TIC.
Promover a melhoria dos sistemas de informação.
Estimular a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar padronização, integridade e segurança.
Promover o atendimento às normas de acessibilidade (e-Mag) e interoperabilidade do Governo Eletrônico (e-Ping), incluindo padrões de governança.
Garantir a segurança da informação e comunicações.
Buscar a melhoria contínua da infraestrutura de TIC.
Manter os processos internos de TIC mapeados, formalizados, mensurados e otimizados.
Promover capacitação/formação de servidores.
Renovar continuamente o parque tecnológico do ITI.

Organização da TI

O ITI é uma autarquia federal vinculada à Casa Civil da Presidência da República, cujo objetivo é manter a Infraestrutura de Chaves Pública Brasileira – ICP-Brasil, sendo a primeira autoridade da cadeia de certificação – AC Raiz.

A Medida Provisória 2.200-2 de 24 de agosto de 2001 deu início à implantação do sistema nacional de certificação digital da ICP-Brasil. Isso significa que o Brasil possui uma infraestrutura pública, mantida e auditada por um órgão público, no caso, o ITI, que segue regras de funcionamento estabelecidas pelo Comitê Gestor da ICP-Brasil, cujos membros, representantes dos poderes públicos, sociedade civil organizada e pesquisa acadêmica, são nomeados pelo Presidente da República.

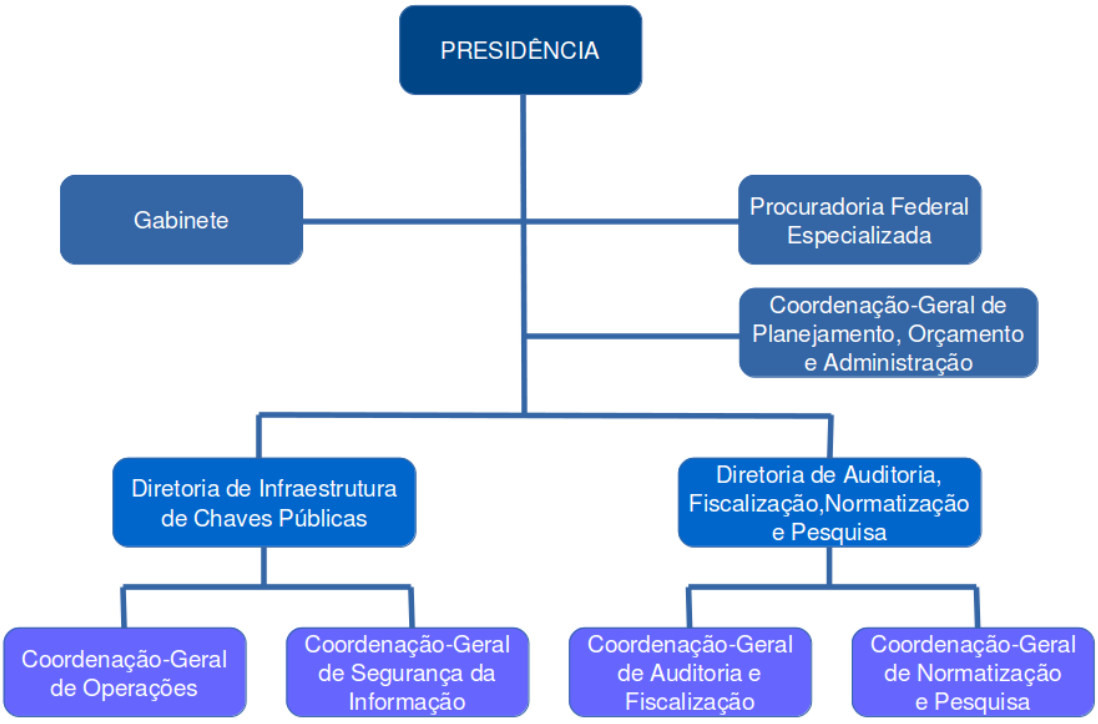
Compete ainda ao ITI estimular e articular projetos de pesquisa científica e de desenvolvimento tecnológico voltados à ampliação da cidadania digital. Sua principal linha de ação é a popularização da certificação digital ICP-Brasil e a inclusão digital, atuando sobre questões como sistemas criptográficos, hardware compatíveis com padrões abertos e

universais, convergência digital de mídias, desmaterialização de processos, entre outras.

De acordo com o artigo 2º do Decreto nº 4.689, de 7 de maio de 2003, o ITI possui a seguinte estrutura organizacional:

> I – órgãos de assistência direta e imediata ao Diretor-Presidente:
>
> a) Gabinete
>
> b) Procuradoria Federal Especializada
>
> II – órgão seccional: Coordenação-Geral de Planejamento, Orçamento e Administração;
>
> III – órgãos específicos singulares:
>
> a) Diretoria de Infraestrutura de Chaves Públicas
>
> b) Diretoria de Auditoria, Fiscalização e Normalização

Organograma do ITI



Áreas Finalísticas

De acordo com o Decreto nº 4.689:

> Art. 7º - À Diretoria de Infraestrutura de Chaves Públicas compete:
>
> I - dirigir a operação da AC Raiz;
>
> II - orientar a elaboração de normas e procedimentos operacionais da AC Raiz e da Segurança da Informação para o ITI;
>
> III - propor a contratação de projetos relativos à operacionalização da AC Raiz, a serem executados com recursos do ITI;
>
> IV - propor a celebração de convênios, acordos, ajustes e de outros instrumentos congêneres de cooperação técnica, no âmbito de sua atuação;
>
> V - coordenar e executar a emissão de certificado para as AC de nível imediatamente subsequente ao da AC Raiz da ICP-Brasil; e
>
> VI - realizar outras atividades determinadas pelo Diretor-Presidente do ITI.
>
> Art. 8º -À Diretoria de Auditoria, Fiscalização e Normalização compete:
>
> I - planejar, coordenar, supervisionar, executar, avaliar e controlar as atividades relacionadas com auditoria, fiscalização e normalização no âmbito da ICP-Brasil e com a definição dos diversos object identifier - OID;
>
> II - atuar como credenciador de empresas de auditoria e auditores independentes para prestação de serviços à ICP-Brasil;
>
> III - propor a celebração de convênios, acordos, ajustes e de outros instrumentos congêneres de cooperação técnica, no âmbito de sua atuação;
>
> IV - elaborar propostas de revisão das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil; e
>
> V - realizar outras atividades determinadas pelo Diretor-Presidente do ITI.

CGPOA

As necessidades básicas de infraestrutura de TI do Instituto são fornecidas e administradas pela CGPOA, a qual compete, de acordo com o art. 6º do Decreto nº 4.689:

> *(…) planejar, coordenar e supervisionar a execução das atividades relacionadas aos Sistemas de Pessoal Civil da Administração Federal - SIPEC, de Organização e Modernização Administrativa - SOMAD, de Administração dos Recursos de Informação e Informática - SISP, de Serviços Gerais - SISG, de Planejamento e de Orçamento Federal, de Contabilidade Federal e de Administração Financeira, no âmbito do ITI.*

De acordo com o art. 3º do Decreto nº 7.579, de 11 de outubro de 2011, integra o SISP

como Órgão Seccional, representada por seu titular, a unidade de administração dos recursos de tecnologia da informação do ITI.

Cabe ressaltar que a ação 6.7 do Planejamento Estratégico do ITI possui como meta a "criação formal de uma área de TIC do Instituto, responsável por agregar valor às soluções de TIC ao negócio", e que objetiva "criar formalmente a área responsável pela TIC institucional, estabelecendo seu regime interno".

CODIS

O Serviço de Controle de Desenvolvimento, Infraestrutura e Suporte – CODIS é a área da CGPOA responsável pelas atividades de gestão da rede, atendimento a usuário e desenvolvimento dos sistemas utilizados pelo ITI.

São reservadas para a CODIS 5 vagas de Analistas em Tecnologia da Informação (ATIs), 1 de GSISP de nível superior e 1 de GSISP de nível médio. Dessas, 4 vagas de ATIs estão preenchidas em 2017.

Referencial Estratégico de TI

De acordo com o Planejamento Estratégico do ITI, disponível em http://www.iti.gov.br/institucional, a missão, a visão, os princípios e valores do ITI são:

Missão do ITI

Atuar na inovação, regulação e provimento de soluções tecnológicas que garantam segurança, autenticidade, integridade e validade jurídica de documentos e transações eletrônicas, respeitando o cidadão, a sociedade e o meio ambiente.

Visão do ITI

Garantir segurança e validade jurídica às transações e documentos eletrônicos, contribuindo também para o desenvolvimento sustentável.

Princípios e Valores do ITI

A proposta de Princípios para o ITI compreende:

- **Segurança** – oferecer soluções que possibilitem a segurança, integridade, autenticidade e confidencialidade em transações e documentos eletrônicos;
- **Validade Jurídica** – cumprir e fazer cumprir todas as normas legais e regulamentares que incidem sobre a Certificação Digital ICP Brasil, de forma que as transações e documentos eletrônicos tenham validade jurídica;
- **Integridade** – garantir que transações e documentos eletrônicos não foram modificados ou destruídos, de maneira não autorizada ou acidental;
- **Autenticidade** – garantir a autoria de transações e documentos eletrônicos;
- **Confidencialidade** – garantir o sigilo de transações e documentos eletrônicos.

O Órgão deve respeitar ainda determinados Valores , que explicitam as crenças e convicções que orientam o comportamento das pessoas e que devem ser defendidas pela Instituição, permeando todas as suas atividades e relações.

A proposta de Valores para o ITI abrange:

- **Credibilidade** – atuar de forma a garantir a Cadeia de Confiança da ICP Brasil no âmbito das entidades que compõem, além de Governo e Sociedade;
- **Agilidade** – entregar resultados com rapidez e qualidade;
- **Ética** – agir com honestidade e lealdade em todas as ações e relações;
- **Inovação** – buscar soluções inovadoras para garantir a segurança em transações e documentos eletrônicos;
- **Transparência** – praticar atos com legalidade, impessoalidade, moralidade, publicidade e eficiência no desempenho de suas atribuições;
- **Responsabilidade Ambiental** – contribuir para a preservação do meio ambiente ao

oferecer soluções que minimizem o uso de recursos naturais e sejam economicamente viáveis, socialmente justas e culturalmente aceitas.

Análise SWOT do ITI (constante do Planejamento Estratégico)

Ambiente Interno	Ambiente Externo
Forças	**Oportunidades**
a) Benefícios da Certificação Digital ICP Brasil: segurança, economicidade, eficiência no uso de recursos, redução de custos, agilidade, integridade, autenticidade, privacidade e validade jurídica em transações e documentos eletrônicos; b) Participação acadêmica em pesquisa científica e desenvolvimento tecnológico; c) Comprometimento e dedicação do quadro de DAS; d) Fomento e apoio tecnológico para o desenvolvimento de novas aplicações; e) Investimento no desenvolvimento de tecnologia nacional na área de segurança da informação; f) Reconhecimento internacional, em especial na América Latina, como órgão de referência em Certificação Digital.	a) A Certificação Digital oferece ganhos em termos de economicidade, agilidade, segurança, validade jurídica em transações e documentos eletrônicos, cada vez mais visíveis, reconhecidas e valorizadas pela sociedade brasileira; b) Alta disponibilidade da ferramenta 24h/7dias/ano, a uma taxa de 99,99%, o que garante seu uso de forma ininterrupta, a qualquer tempo e independente de sua localização; c) Crescente oferta de novas aplicações que se utilizam da Certificação Digital como ferramenta de segurança e validade jurídica tanto no âmbito governamental como privado; d) Ampla gama de aplicações públicas e privadas com potencial para uso da ferramenta; e) Amplo desenvolvimento do *e-commerce* alicerçado no uso de certificado digital ICP – Brasil; f) Incentivo à desmaterialização de processos, por conta da assinatura do Acordo de Cooperação Técnica com a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento (SLTI/MPOG), que tem como objetivo a modernização e desburocratização da administração pública federal, a partir da implementação do Plano Nacional de Desmaterialização de Processos – PNProc; g) O uso da Certificação Digital tem se revelado uma alternativa para a redução do custo Brasil e efetiva

	contribuição para a sustentabilidade ("*Green Economy*"), ao viabilizar ações que reduzem o consumo de papel, tinta, madeira e água; e h) Desconhecimento da sociedade quanto aos benefícios da ferramenta.
Ambiente Interno	**Ambiente Externo**
Fraquezas	**Ameaças**
a) Estrutura organizacional e orçamentária defasada, haja vista que o Instituto ainda opera com a mesma estrutura organizacional desde sua criação em 2002 e não dispõe de quadro de carreira e quadro de funcionários próprio, obrigando-o a valer-se de serviços terceirizados, que muitas vezes têm alcance limitado e forte impacto nas despesas discricionárias de seu orçamento. Áreas críticas, como a de controle da infraestrutura de comunicações, redes, sistemas e segurança da informação da área meio sofrem com ausência de profissionais próprios e suficientes para a sua gestão. Na área finalística, essa limitação vai ainda além, retardando avanços na área de pesquisa e desenvolvimento. Uma vez que os recursos são alocados prioritariamente na operacionalização da Infraestrutura de Chaves Públicas, haja vista sua alta disponibilidade (24h/7dias/ano – 99.99%); b) Carência de profissionais especializados na área de pesquisa em C&T e Desenvolvimento Tecnológico, o que obriga o Instituto a valer-se de Acordos de Cooperação e Termos de Descentralização de Créditos para garantir a compatibilidade do sistema com avanços de novas Tecnologias da Informação;	a) Estrutura operacional e orçamentária defasada, haja vista que o Instituto ainda opera com a mesma estrutura organizacional desde sua criação em 2002 e não dispõe de quadro de carreira e quadro de funcionários próprio, obrigando-o a valer-se de serviços terceirizados, que muitas vezes têm alcance limitado e forte impacto nas despesas discricionárias de seu orçamento; b) Permanente avanço tecnológico em segurança da informação, o que exige cada vez mais investimentos em pesquisa e desenvolvimento de novas tecnologias voltadas a garantir interoperabilidade e segurança em transações e documentos eletrônicos; c) Avanço do uso da Certificação Digital em processos críticos para a sociedade brasileira, o que impõe permanente monitoramento de ataques, fraudes, e outras tentativas de invasão de sistemas computacionais; d) Significativo crescimento da Infraestrutura de Autoridades Certificadoras e Prestadores de Serviços, o que exige cada vez mais recursos humanos, físicos e lógicos capazes de auditar e fiscalizar essa rede, como forma de garantir sua conformidade a padrões e procedimentos estabelecidos pela ICP – Brasil; e e) Desconhecimento da sociedade quanto aos benefícios da ferramenta.

c) Ausência de sede própria para integração do ambiente seguro. Atualmente o Órgão ocupa um prédio monousuário alugado, sendo obrigado a manter a sala cofre nas dependências da Presidência da República, o que torna sua administração mais cara e complexa; d) Alta demanda de monitoramento do sistema com relação a tentativas de invasão e fraudes, permanente investimento em interoperabilidade e crescente demanda por homologação de artefatos; e e) Alta demanda para pesquisa e alinhamento de padrões e normas internacionais, com vista à interoperabilidade.	

Missão da CODIS

Prover soluções de Tecnologia da Informação e Comunicação com elevado padrão de qualidade e segurança, contribuindo para atingir a missão estratégica do ITI com eficácia, eficiência e excelência.

Visão da CODIS

Ser reconhecida como provedora de Soluções inovadoras que agreguem valor ao Instituto, contribuindo para que os objetivos estratégicos sejam alcançados com excelência por meio da gestão e melhoria contínua dos processos."

Valores da CODIS

A CODIS é direcionada pelos seguintes valores:

- Compromisso com a ética e com a transparência;
- Obediência às normas vigentes;

- Respeito aos clientes;
- Cooperação;
- Governança corporativa com foco em Tecnologia da Informação
- Compromisso com segurança de dados;
- Eficiência;
- Profissionalismo;
- Inovação;
- Responsabilidade Ambiental;
- Autodesenvolvimento.

Análise SWOT da TI meio (CODIS)

Foco 1: o uso da gestão de TI

Ambiente interno (referente à CODIS)	Ambiente externo (externo à CODIS)
Forças	**Oportunidades**
● existência do PDTIC 2013-2014 ● existência de procedimentos e normas formalizados (Normas de Controle de Acesso Lógico e Processo de Desenvolvimento de Sistemas - PDS) ● serviço de Suporte à usuário e Administração de Redes eficientes ● ambiente de trabalho agradável ● sinergia e motivação da equipe de trabalho ● equipe certificada em Cobit e ITIL (certificação *Foundation*) ● alinhamento das contratações de TI com os processos da Instrução Normativa 04/2010 SLTI/MPOG ● adoção inicial das melhores práticas de mercado (Cobit, PMBoK, ITIL) ● aproximação entre área fim e área meio	● apoio da alta administração às atividades da CODIS ● existência do Planejamento Estratégico do ITI, direcionando as ações da CODIS ● existência do Comitê Estratégico de TI ● existência da POSIC do ITI ● previsão de reestruturação do Instituto ● aproximação com as demais áreas do ITI ● processo de contratação de soluções de TI mapeado e definido pela Instrução Normativa 04/2010 SLTI/MPOG ● papel atuante do TCU, AGU, SLTI e órgãos de controle forçando a importância da governança de TI ● ferramental disponibilizado pelo SISP (portal do governo eletrônico, FAQ, Catálogo de Serviços)

• fornecimento de serviços ao Instituto	• levantamento anual e avaliação de Governança do TCU • existência Lei de Acesso à Informação (LAI) • existência do projeto PNDProc – Administração Sem Papel • ação 6.7 do Planejamento Estratégico de TI do órgão – "criação formal de uma área de TIC do Instituto, responsável por agregar valor às soluções de TIC ao negócio" • existência do Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação do TCU
Fraquezas	**Ameaças**
• não há definição formal das atividades e responsabilidades da área • não há direcionamento estratégico formalizado para a área • nem todos os processos e procedimentos da área estão documentados • aderência aos modelos de melhores práticas (Cobit, PMBoK, ITIL) ainda está em estágio inicial • falta capacitação em Segurança da Informação • falta consolidação do relacionamento com as outras áreas do Instituto • poucas normas de utilização da infraestrutura foram instituídas • serviço de desenvolvimento de sistemas é inexistente • datacenter não é protegido por sistema de segurança física	• resistência natural a mudanças propostas pela CODIS • comitê de Segurança da Informação não atuante • cultura de governança de TI não consolidada no órgão • área de TI meio não institucionalizada – não existe formalmente na atual estrutura do ITI • inexistência de um ato formalizando o processo de contratação de TI no âmbito do ITI • a área não é alçada como estratégica pelo órgão • Observância a normas, padrões e procedimentos instituídos pela CODIS não é total • Dificuldade de atendimento a todas as exigências da IN-4/SLTI por limitação

	organizacional do instituto ● contingenciamento orçamentário ● ausência de quadro próprio de funcionários do órgão ● ausência de comunicação formal pelas demais áreas em relação as atualizações das informações mantidas em nossos banco de dados ● Cronograma e prioridades definidos sem levar em consideração a capacidade organizacional da CODIS ● arquitetura de infraestrutura é diversificada nas áreas do Instituto

Foco 2: o uso da Tecnologia

Ambiente interno	Ambiente externo
Forças ● utilização de software livre ● segurança dos dados em relação a: confidencialidade, integridade, e controle de acesso ● utilização de ferramentas de gerenciamento de projetos ● resiliência, alta disponibilidade e conformidade do Datacenter	**Oportunidades** ● política de massificação do uso do certificado digital no ITI ● existência de usuários com conhecimento avançado em TI
Fraquezas ● uso incipiente de tecnologias de GED e certificação digital ● limitações inerentes ao software livre ● segurança dos dados em relação a auditoria e rastreabilidade ● pouca automatização de processos	**Ameaças** ● rápida evolução tecnológica dos equipamentos de TI

• perda de garantia dos equipamentos • impressoras fora de garantia e sem manutenção • não há gerência de impressão • solução de virtualização licitada mas não adquirida • solução incipiente de armazenamento de dados em rede • processos pouco automatizados • falta de administração de bancos de dados	

Resultados do PDTIC de 2016

Os resultados alcançados a partir da realização dos projetos e ações do Planejamento de TI de 2015-2016 estão também listados no Anexo I, na coluna executados em 2016. Os demais projetos sem a informação de execução não foram concluídos ou iniciados por falta de recurso orçamentário, e permanecem planejados para o exercício de 2017-2018.

Inventário de necessidades 2017-2018

O inventário das necessidades do ITI, com eventual priorização do CETI, mas com a classificação das demandas segundo a matriz GUT, estão listados no Anexo I.

A priorização das necessidades conforme disponibilidade orçamentária será tratada em reunião do CETI, para aprovação e delimitação das prioridades conforme Planejamento Estratégico 2015-2018, quando de disponibilidade de recursos financeiros, e aprovação da Diretoria Colegiada.

Processo de Revisão do PDTIC

As priorizações de 2017 serão revisadas obrigatoriamente semestralmente, ou quando solicitado pelo CETI.

Fatores Críticos para Implantação do PDTIC

Os pontos chaves que definem o sucesso ou o fracasso do PDTIC 2017-2018 são:

- Possuir orçamento para execução das ações priorizadas;
- Obediência às prioridades aprovadas pelo CETI;
- Monitoramento e controle das ações listadas e priorizadas neste documento.

Conclusão

De acordo com o Cobit 4.1, “a governança de TI integra e institucionaliza boas práticas para garantir que a área de TI da organização suporte os objetivos de negócio.” Desta forma, as ações de TI devem estar alinhadas aos objetivos estratégicos, para que as expectativas da organização sejam atingidas.

O Instituto está amadurecendo sua governança em TI e prova disso é a publicação do seu Planejamento Estratégico, a atuação do Comitê de TI e a elaboração deste PDTIC.

ITI
Instituto Nacional de Tecnologia da Informação

ANEXO 1 – Inventário de necessidades 2017/2018

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

GABINETE

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
1	Atualização do SGC da ICP-Brasil	CONTRATAÇÃO DE TI	Evolução tecnologica da família SGC – Ywyra/Ywapa/Hawa	Objetivo 4.2	DINFRA	DINFRA	DINFRA	5	5	5	125	PRIORIZADO - 2017	R$ 64.200,00	R$ 250.000,00	R$ 262.500,00	R$ 275.625,00	TDC UFSC
2	Atualização do Assinador de Referência v.3 com incorporação do Plugin PADES	CONTRATAÇÃO DE TI	Atualização do Assinador a partir do novo padrão PADES	Objetivo 5.2	DINFRA	DINFRA DAFN	DINFRA	5	5	4	100	PRIORIZADO - 2017	R$ 0,00	R$ 200.000,00	R$ 210.000,00	R$ 220.500,00	TDC UnB
3	Atualização do Verificador de Conformidade	CONTRATAÇÃO DE TI	Evolução tecnologica CADES e XADES e adoção do PADES e melhorias do verificador de conformidade	Objetivo 5.2	DINFRA	ITI	DINFRA	5	5	5	125	PRIORIZADO - 2017	R$ 41.850,00	R$ 50.000,00	R$ 52.500,00	R$ 55.125,00	TDC UFSC
4	Atualização do Gerador de Políticas	CONTRATAÇÃO DE TI	Atualização do Gerador de políticas a partir das correções no DOC-ICP-15	Objetivo 5.2	DINFRA	ITI	DINFRA	5	5	5	125	PRIORIZADO - 2017		R$ 50.000,00	R$ 52.500,00	R$ 55.125,00	TDC UFSC
5	Cloud Computing ITI	SERVIÇO DE TI	Definição de ferramentas de cloud computing para uso interno no ITI	Objetivo 7.11	ITI	CODIS	ESCOLHA:	3	4	4	48	DEMANDAS FUTURAS		0,00	0,00	0,00	
6	Serviços Avançados para Gestão de Conhecimento	SERVIÇO DE TI	Definição de ferramentas de gestão de conhecimento (Wiki, SEI, etc)	Objetivo 7.11	ITI	CODIS	ESCOLHA:	3	4	4	48	DEMANDAS FUTURAS		0,00	0,00	0,00	
7	Solução de edição de imagens e video	CONTRATAÇÃO DE TI	Aquisição de ferramentas de editoração eletrônica (hardware e software)	Objetivo 6.2	GABINETE	ASCOM CODIS	ESCOLHA:	3	4	4	48	DEMANDAS FUTURAS		R$ 80.000,00	R$ 50.000,00	R$ 50.000,00	
8	Atualização do SGCA	CONTRATAÇÃO DE TI	Evolução tecnológica do SGCA (assinador de certificado de atributos)	Objetivo 5.2	GABINETE	ASCOM CODIS	ESCOLHA:	3	4	4	48	DEMANDAS FUTURAS		R$ 150.000,00	R$ 150.000,00	R$ 180.000,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

	ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
									GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
DAFN	1	Manutenção do SDK que valida certificados	INFRAESTRUTURA DE TI	Atualização do SDK que realiza a identificação e validação de certificados digitas. Este software encontra-se defasado com os novos drivers e versões de certificados.	Objetivo 2.1	CGAF	ITI	DAFN	5	5	5	125	CONTRATADO - 2025	R$ 18.500,00	R$ 19.583,64	R$ 20.000,00	R$ 22.000,00	06/2015
	2	Aquisição de Sete Notebooks para auxiliar os trabalhos de auditoria	INFRAESTRUTURA DE TI	Atualização do parque tecnológico, a partir do Estabelecimento de uma política de atualizações de equipamentos, a fim de Manter o parque computacional em Produção atualizado e em garantia.	Objetivo 2.1	CGAF	CGAF	DAFN	4	4	5	80	DEMANDAS FUTURAS		R$ 28.000,00	R$ 32.000,00	R$ 32.000,00	
	3	Aquisição de dois servidores para auxiliar os trabalhos de auditoria	INFRAESTRUTURA DE TI	Possibilitar o processamento das informações mantidas para realização das tarefas de auditorias bem como manter as informações dos certificados para analises e fiscalizações.	Objetivo 2.1	CGAF	CGAF	DAFN	5	4	4	80	DEMANDAS FUTURAS		R$ 65.000,00			
	4	Aquisição software SGBD para manter as informações dos serviços de auditoria	INFRAESTRUTURA DE TI	Possibilitar o armazenamento e processamento das informações mantidas para realização das tarefas de auditorias bem como manter as informações dos certificados para analises e fiscalizações.	Objetivo 2.1	CGAF	CGAF	DAFN	5	4	5	100	DEMANDAS FUTURAS		R$ 60.000,00			
	5	Contratação de Fábrica de Software – (Websys) Manutenção	CONTRATAÇÃO DE TI	Contratação de fábrica de software em pontos de função Para a manutenção dos softwares da DAFN	Objetivo 2.1	DAFN	ITI	ESCOLHA:	5	5	5	125	CONTRATADO - 2017	R$ 493.026,89 *	R$ 213.500,00	R$ 512.400,00	R$ 512.400,00	27/2014
	6	Aquisição de Software para edição de arquivos no ASN.1.	INFRAESTRUTURA DE TI	Os arquivos de políticas de assinatura disponibilizados pelo ITI são gerados no padrão ASN.1. Com a falta de ferramentas o ITI fica na dependência de colaboradores externos para atualizar esses arquivos. A utilização deste tipo de ferramenta traria mais autonomia para o ITI nestas operações.	Objetivo 2.1	CGNP	DAFN	DAFN	5	5	5	125	DEMANDAS FUTURAS		R$ 2.000,00	R$ 300,00	R$ 300,00	
	7	Manutenção do contrato de Link de Internet (Infovia) – SERPRO.	CONTRATAÇÃO DE TI	Aquisição / manutenção do contrato em vigor para garantir acesso à INFOVIA (Sistemas Estruturantes do Governo), assim como serviços necessários para o bom andamento das atividades cotidianas do ITI.	Objetivo 7.10	CGPOA	ITI	DAFN	4	4	4	64	CONTRATADO - 2017	###	R$ 170.337,12	R$ 178.853,98	R$ 187.796,67	04/2015
	8	Aquisição de licenças de software para análise de dados de auditoria	SERVIÇO DE TI	Documentar o mapeamento das áreas organizacionais, de processos, riscos e controles. Ele possibilita, também que sejam feitas análises de riscos periódicas, gerenciamento de planos de ação, planejamento de trabalhos, testes de controles, coleta de perdas, registro de incidentes, acompanhamento de indicadores de riscos e geração de relatórios.	Objetivo 2.1	DAFN	DAFN	DAFN	4	4	3	48	PRIORIZADO - 2017		R$ 86.000,00			
	9	Aquisição de licenças de software para manipulação de arquivos *Portable Document Format*	SERVIÇO DE TI	Nas atividades da CGNP estão incluídas rotinas que demandam a manipulação de arquivos PDF. Por exemplo, a disponibilização da pauta de resoluções para o Comitê Gestor, em um arquivo único por demanda, contendo todos os artefatos envolvidos, conforme solicitado pelo Secretário-Executivo, envolve a junção e a edição de arquivos PDF que só é possível utilizando um editor PDF. Além disso, os scanners disponíveis no ITI produzem documentos não indexados, sem OCR, o que impossibilita a busca de palavras chave nesses documentos e que podem ser tratados por editores de PDF.	Objetivo 2.1	CGAF	ITI	DAFN	4	3	5	60	PRIORIZADO - 2017		R$ 50.000,00			
	10	Aplicação analítica para tomada de decisão	SERVIÇO DE TI	Verifica-se uma crescente necessidade de análise de dados obtidos pelo cadastramento, auditorias e envio de informações dos agentes cadastrados. Nesse sentido, a construção de aplicações analíticas que auxiliaram os diretores nas tomadas de decisão se faz necessária. Este tipo de aplicação possibilita aos usuários a descoberta de dados e relações que muitas vezes estão ocultas em relatórios estáticos, apresentando tendências e conexões de relacionamentos entre os dados disponíveis.	Objetivo 2.1	DAFN	ITI	DAFN	5	5	5	125	PRIORIZADO - 2017		R$ 150.000,00	R$ 50.000,00	R$ 50.000,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
1	Manutenção preventiva e corretiva do ambiente seguro (ongoing) – ACECO.	SERVIÇO DE TI	Manutenção preventiva e corretiva do ambiente seguro da AC Raiz. ACECO	Objetivo 1.2	CGSI	CGSI	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 1.087.140,00	R$ 1.195.854,00	R$ 1.315.439,40	17/2013
2	Manter a manutenção preventiva e corretiva para os equipamentos da Bry (Serviço continuado).	CONTRATAÇÃO DE TI	Contratação que visa manter a manutenção preventiva e corretiva para os equipamentos da EAT.	Objetivo 1.5	CGO	DINFRA	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 138.590,28	R$ 300.000,00		04/2013
3	Manter a manutenção preventiva e corretiva para os equipamentos da Symmetricom/Ncipher (serviço continuado) – Thales	CONTRATAÇÃO DE TI	Contratação que visa manter a manutenção preventiva e corretiva para os equipamentos da EAT. Thales.	Objetivo 1.5	CGO	DINFRA	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 255.257,88	R$ 600.000,00		03/2013
4	Manutenção de HSM (Serviço Continuado) – Kryptus.	CONTRATAÇÃO DE TI	Contratação de serviço continuado que visa manter a estrutura da Autoridade Certificadora da ICP-Brasil. Kryptus.	Objetivo 1.1	CGO	DINFRA	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 506.500,00	R$ 557.150,00		15/2014
5	Serviço de acesso a Infovia Brasília provido pelo SERPRO.	SERVIÇO DE TI	Serviço de acesso à Infovia Brasília provido pelo Serpro.	Objetivo 1.2	CGSI	CGSI	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 170.337,12	R$ 187.370,83	R$ 206.107,92	04/2015
6	Manutenção e operação do sítio de contingência da AC-Raiz (UFSC).	SERVIÇO DE TI	Acordo de cooperação técnica que viabiliza o site de contingência em SC da AC Raiz.	Objetivo 1.3	CGSI	CGSI	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 1.098.000,00	R$ 1.207.800,00	R$ 1.328.580,00	01/2013
7	Enlace de comunicação de dados através da rede RNP	SERVIÇO DE TI	Serviço de acesso à RNP (não há custo de contratação)	Objetivo 1.3	CGSI	CGSI	ESCOLHA:	5	5	4	100	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
8	Manutenção da solução de storage – COMPWIRE.	INFRAESTRUTURA DE TI	Considerando o contingenciamento orçamentário do ITI optou-se por contratar apenas a manutenção preventiva e corretiva do storage atual (ambos) – Compwire.	Objetivo 4.1	CGSI	CGSI	DINFRA	5	5	4	100	CONTRATADO - 2017	###	R$ 167.134,32	R$ 183.847,75	R$ 202.232,53	07/2015
9	Auditoria independente para AC-Raiz – TI	CONTRATAÇÃO DE TI	Avaliar e adequar as operações da AC Raiz em conformidade com os normativos da ICP-Brasil e demais normativos internacionais.	Objetivo 1.6	ITI	ITI	DINFRA	5	5	4	100	CONTRATADO - 2017	R$ 211.849,92	R$ 211.849,92	R$ 233.034,91	R$ 256.338,40	
10	Aquisição de nova solução de storage	INFRAESTRUTURA DE TI	Aquisição de nova solução de storage (armazenamento) tendo em vista que, apesar do ITI ter contrato de manutenção da solução existente com a empresa COMPWIRE, os equipamentos atuais se encontram em final do seu ciclo de vida, sendo necessária a aquisição de nova solução	Objetivo 4.1	CGSI	CGSI	DINFRA	5	5	4	100	DEMANDAS FUTURAS		R$ 900.000,00	0,00		
11	Manutenção ou adequação do parque de equipamentos:fitoteca	INFRAESTRUTURA DE TI	Contratação de empresa especializada para manutenção de servidores, switches e fitoteca com garantia que venham expirar e\ou adequação continua do parque de equipamentos	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	5	5	4	100	DEMANDAS FUTURAS		R$ 120.000,00	-	-	
12	Manutenção ou adequação do parque de equipamentos:servidores	INFRAESTRUTURA DE TI	Contratação de empresa especializada para manutenção de servidores, switches e fitoteca com garantia que venham expirar e\ou adequação continua do parque de equipamentos	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	5	5	4	100	DEMANDAS FUTURAS		R$ 60.000,00	-	-	
13	Manutenção e Evolução de *software* para manipulação de documentos assinados digitalmente no padrão PAdES ICP-Brasil.	INFRAESTRUTURA DE TI	Manutenção e Evolução do *Plugin PAdES ICP-Brasil.*	Objetivo 3.1	CGNP	ITI	DINFRA	5	5	4	100	DEMANDAS FUTURAS	R$ 59.550,00	R$ 150.000,00	R$ 60.000,00	R$ 60.000,00	
14	Atualização tecnológica dos subsistemas do ambiente seguro do ITI (SALA COFRE)	INFRAESTRUTURA DE TI	Adequar os subsistemas, mantendo a garantia e suporte continuados dos fabricantes: -Adequação tecnológica do subsistema de climatização e energia -Adequação tecnológica do subsistema de detecção e combate à incêndio -Adequação tecnológica do subsistema de supervisão e controle	Objetivo 1.4	CGSI	CGSI	ESCOLHA:	5	4	4	80	DEMANDAS FUTURAS		R$ 500.000,00	R$ 550.000,00	R$ 605.000,00	
15	Enlace de comunicação de dados de Internet	SERVIÇO DE TI	Hoje dispomos de 2 links: infovia e RNP, sendo que o acesso à RNP depende de uma saída através da INFOVIA. Para garantir redundância real no acesso à Internet da AC Raiz de Brasília é necessário a contratação de link de dados adicional.	Objetivo 1.2	CGSI	CGSI	ESCOLHA:	5	4	4	80	DEMANDAS FUTURAS		R$ 180.000,00	R$ 198.000,00	R$ 217.800,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

	ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
									GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
DINFRA	16	Instalação do nível 3 no prédio do ITI (NOC)	INFRAESTRUTURA DE TI	Em andamento (verificação de viabilidade). Meta no mapa estratégico: (Adequação das instalações técnicas da DINFRA e do CPD do ITI e instalação de solução de monitoramento remoto (NOC)). Visa promover o aprimoramento da gestão do ambiente seguro permitindo gerenciamento a partir do prédio do ITI. Atualmente as intervenções no ambiente exigem deslocamentos constantes ao anexo 3 da presidência da república.	Objetivo 1.4	DINFRA	CGSI/CGO	ESCOLHA:	5	4	4	80	DEMANDAS FUTURAS			R$ 650.000,00	-	
	17	Balanceador de link	INFRAESTRUTURA DE TI	Tem o objetivo de otimizar o uso dos links de dados na entrada e saída, além de melhorar a gestão de disponibilidade.	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	5	4	4	80	DEMANDAS FUTURAS		R$ 150.000,00	R$ 165.000,00	R$ 181.500,00	
	18	Serviço de administração de rede – COOPERSYSTEM.	CONTRATAÇÃO DE TI	Contratação que visa a administração dos equipamentos servidores e demais atividades afetas. Coopersystem.	Objetivo 7.12	CGPOA	CGPOA	DINFRA	5	4	4	80	CONTRATADO - 2017	###	R$ 172.212,48	R$ 180.823,10	R$ 189.864,26	17/2011
	19	Serviço de suporte técnico de apoio a operação do ambiente seguro	CONTRATAÇÃO DE TI	Contratação de suporte técnico para manutenção e operação da infraestrutura de rede e demais serviços da AC Raiz.	Objetivo 1.2	DINFRA	DINFRA	ESCOLHA:	5	5	3	75	DEMANDAS FUTURAS			R$ 871.200,00	R$ 958.320,00	
	20	Serviço de Atendimento ao usuário do ITI – DIGISYSTEM.	CONTRATAÇÃO DE TI	Contratação que visa o atendimento ao usuário lotado no ITI e atividades correlatas. Digisystem.	Objetivo 7.12	CGPOA	ITI	DINFRA	4	4	4	64	CONTRATADO - 2017	###	R$ 212.378,40	R$ 222.997,32	R$ 234.147,19	02/2015
	21	Infraestrutura de Carimbo de Tempo	CONTRATAÇÃO DE TI	Contratação que visa ampliar a disponibilidade da EAT.	Objetivo 1.5	CGO	DINFRA	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS			R$ 1.500.000,00		
	22	Realizar Acordo de Cooperação Técnica entre o ITI e o INMETRO	CONTRATAÇÃO DE TI	Convênio que visa obter o Apoio do INMETRO ao ambiente de Rastreabilidade da FCT-ICP-Brasil.	Objetivo 1.5	CGO	DINFRA	ESCOLHA:	5	4	3	60	DEMANDAS FUTURAS		0,00	0,00		
	23	Solução de gerenciamento de segurança	INFRAESTRUTURA DE TI	Aprimoramento dos recursos de segurança do perímetro de rede da ACRAIZ	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	3	4	3	36	DEMANDAS FUTURAS			R$ 700.000,00	R$ 770.000,00	
	24	Estação computacional de trabalho	INFRAESTRUTURA DE TI	Estações operacionais com necessidades diferenciadas de recursos computacionais para atender demandas que exigem maior capacidade de processamento, memória e periféricos	Objetivo 4.1	DINFRA	DINFRA	ESCOLHA:	4	3	3	36	DEMANDAS FUTURAS			R$ 45.000,00	-	
	25	Criação/implantação de ACT do ITI	INFRAESTRUTURA DE TI	Contratação que visa ampliar a atuação da EAT.	Objetivo 1.5	CGO	DINFRA	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS			R$ 1.500.000,00		
	26	Laboratório Forense	INFRAESTRUTURA DE TI	Contratação de sistema que permita melhorar a infraestrutura de investigação forense do ITI.		DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS			R$ 500.000,00		
	27	Desenvolvimento de Midleware para dispositivos criptográficos (cartão, token, memória, etc).	CONTRATAÇÃO DE TI	Elaboração de projeto e desenvolvimento de sistema para interação com mídias inteligentes.	Objetivo 5.2	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS			R$ 700.000,00		
	28	Desenvolvimento de Protocolo para Carimbo de Tempo.	CONTRATAÇÃO DE TI	Elaboração de projeto e desenvolvimento de sistema para Auditoria e Sincronismo de equipamentos da Rede de Carimbo do Tempo.	Objetivo 5.2	'	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS			R$ 700.000,00		

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
29	Contratar empresa especializada para ministrar treinamentos	PESSOAL DE TI	Capacitação COBIT, cujo objetivo principal é prover um conjunto de diretrizes para processos, práticas e controles, voltado para redução de risco, que enfoca integridade, confiabilidade e segurança. Suas recomendações buscam um modelo de maturidade em governança para auxiliar no cumprimento dos objetivos da organização.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação ITIL, cujo objetivo é promover o alinhamento estratégico entre as áreas de negócio e as áreas de TI das organizações.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação PMBOK, cujo objetivo principal é proporcionar os conhecimentos necessários para melhor integrar os elemento de um projeto, seu escopo, riscos e demais fases.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em Gestão, Mapeamento e Auditoria da Informação e do Conhecimento, com o objetivo de proporcionar o alinhamento da informação e do conhecimento com os objetivos estratégicos do ITI.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em Gestão de Continuidade de Negócios – Aborda os princípios, conceitos, objetivos e práticas decorrentes da Norma BS 25999, incluindo a implementação de um sistema de gestão e o desenvolvimento dos planos de continuidade, recuperação e gerência de incidentes.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em Habilidades Consultivas para Profissionais de Segurança – Objetivo em adquirir um conjunto de habilidades de consultoria essenciais para as atividades do ITI, organizadas com base nas quatro etapas do ciclo de vida dos projetos.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação Módulo Risk Manager – Básico e Avançado – Apresenta os conceitos essenciais para a utilização do produto, suas funcionalidades, casos práticos de uso e exercício de fixação.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em fundamentos da NBR ISO 31000:2009 - oferecer aos participantes a oportunidade conhecer a norma e os elementos que baseados nela compõem um Sistema de Gestão de Riscos.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em metodologia de gestão de processos. Ampliar e melhorar os serviços prestados pela área e obter competências essenciais para o alcance da meta	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Capacitação em Sistema de Gestão de Segurança da Informação — NBR ISO/TEC 27000, 27001, 27002, 27003, 27004 e 27005.	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	BPM - Business Process Management – Gerenciamento de Processo – Capacitação em metodologia de gestão de processos. Ampliar e melhorar os serviços prestados pela área e obter competências essenciais para o alcance da meta	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Curso especializado em Segurança da Informação Aplicada	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
		PESSOAL DE TI	Curso preparatório para Certificação em CISSP ® - Certified Information Systems Security Professional	Objetivo 7.4	DINFRA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 20.000,00	R$ 20.000,00		
30	Manutenção ou adequação do parque de equipamentos: switches	INFRAESTRUTURA DE TI	Contratação de empresa especializada para switches com garantia que venha expirar e\ou adequação continua do parque de equipamentos	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	4	3	2	24	DEMANDAS FUTURAS			R$ 60.000,00	R$ 66.000,00	
31	Solução de virtualização	INFRAESTRUTURA DE TI	Prospecção e eventual aquisição de software de virtualização para o ambiente seguro principal/contingência.	Objetivo 4.1	CGSI	CGSI	ESCOLHA:	3	3	2	18	DEMANDAS FUTURAS			R$ 1.500.000,00	-	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
1	Aquisição de Certificado Digital	CONTRATAÇÃO DE TI	Aquisição de Certificado Digital para a renovação dos emitidos para a Autarquia desde 2013	Objetivo 5.1	CGPOA	ITI	ESCOLHA:	5	5	4	100	PRIORIZADO - 2017		R$ 50.000,00	R$ 50.000,00	R$ 50.000,00	
2	Serviço de Monitoramento de incidentes	CONTRATAÇÃO DE TI	Contratação de serviço de análise e acompanhamento dos riscos referentes á área meio do Instituto	Objetivo 7.13	CGPOA	CGPOA	ESCOLHA:	5	4	4	80	DEMANDAS FUTURAS		R$ 200.000,00	R$ 200.000,00	R$ 200.000,00	
3	Manutenção do link de internet redundante/contingência	CONTRATAÇÃO DE TI	Aquisição / manutenção do contrato em vigor para garantir acesso redundante à internet, assim como prover os serviços necessários para o bom andamento das atividades cotidianas do ITI	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	5	4	4	80	CONTRATADO - 2017	R$ 95.900,04	R$ 95.900,04	R$ 100.695,04	R$ 105.729,79	06/2017
4	Manutenção do contrato de Empresa Claro S/A – móvel	SERVIÇO DE TI	Prestação de serviços de telefônico móvel (SMP móvel fixo e móvel – móvel), nas modalidades longa distância Nacional LDN e Longa Distância Internacional LDI. Contrato n. 03/2012 Deixou de existir em MARÇO/2017.	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	ESCOLHA:	R$ 528,12	-	-	-	03/2017
5	Manutenção do contrato de Empresa OI S/A – móvel	SERVIÇO DE TI	Contratação de empresa especializada na prestação de serviços especializado telefônico móvel pessoal, com fornecimento de 30 aparelhos celulares em regime de comodato. Contrato n. 27/2012	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	CONTRATADO - 2017	R$ 14.869,24	R$ 66.595,32	R$ 69.925,09	R$ 73.421,34	27/2012
6	Manutenção do contrato de Empresa OI S/A – fixo	SERVIÇO DE TI	Prestação de serviço telefônico fixo comutado-longa distância nacional a partir do tronco DDR para linhas fixas e móveis de longa distância nacional Contrato n. 23/2013	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	CONTRATADO - 2017	R$ 4.583,68	R$ 12.837,06	R$ 13.478,91	R$ 14.152,86	23/2013
7	Manutenção do contrato de Empresa OI S/A – fixo	SERVIÇO DE TI	Prestação de serviço telefônico fixo comutado-longa distância Internacional, a partir de tronco fixo, para linhas fixas e moveis de longas distâncias internacional para os países Suíça, Argentina, Estados Unidos, França, Itália, Peru, Portugal, Reino Unido, Chile e Paraguai. Contrato n. 24/2013	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	CONTRATADO - 2017	R$ 93,04	R$ 33.175,04	R$ 34.833,79	R$ 36.575,48	24/2013
8	Manutenção preventiva e corretiva da Central Privada de Comutação Telefônica do tipo PABX – SOPHO	SERVIÇO DE TI	Manutenção preventiva e corretiva da Central Privada de Comutação Telefônica do tipo PABX.	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	CONTRATADO - 2017	R$ 12.863,60	R$ 14.590,80	R$ 15.320,34	R$ 16.086,36	26/2014
9	Manutenção do contrato de Empresa OI S/A – fixo	SERVIÇO DE TI	Prestação de serviço telefônico Fixo comutado-ligações locais. Contrato n. 08/2015	Objetivo 7.10	CGPOA	ITI	CGPOA	5	4	4	80	CONTRATADO - 2017	R$ 25.811,08	R$ 58.795,47	R$ 61.735,24	R$ 64.822,01	08/2015
10	Segurança do DataCenter da CODIS	INFRAESTRUTURA DE TI	Consiste na adequação do DataCenter da CODIS aos níveis mínimos de Segurança necessários para a sua boa utilização	Objetivo 7.13	CGPOA	CGPOA	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 350.000,00	R$ 250.000,00	R$ 150.000,00	
11	Adequação elétrica do DataCenter da CODIS	INFRAESTRUTURA DE TI	Consiste na adequação elétrica necessária para o bom funcionamento do DataCenter da CODIS	Objetivo 7.13	CGPOA	CGPOA	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 200.000,00	R$ 100.000,00	R$ 100.000,00	
12	Adequação climática do DataCenter da CODIS	INFRAESTRUTURA DE TI	Consiste na adequação climática do DataCenter da CODIS às boas práticas no que diz respeito a refrigeração de Datacenter	Objetivo 7.13	CGPOA	CGPOA	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 200.000,00	R$ 0,00	R$ 0,00	
13	Serviço de manutenção da rede lógica e elétrica	SERVIÇO DE TI	Planejamento e contratação de empresa especializada em manutenção da rede lógica e elétrica da autarquia	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 40.000,00	R$ 42.000,00	R$ 44.100,00	
14	Ampliação do Storage	CONTRATAÇÃO DE TI	Aquisição de discos e gavetas para ampliar o Storage administrado pela CODIS com o intuito de melhor atender as demandas do ITI	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 300.000,00	R$ 250.000,00	R$ 200.000,00	
15	Atualização do parque tecnológico de Desktops	CONTRATAÇÃO DE TI	Atualização do parque tecnológico, a partir do estabelecimento de uma política de atualizações de equipamentos, a fim de manter o parque computacional em produção atualizado e em garantia.	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	4	4	4	64	PRIORIZADO - 2017		R$ 150.000,00	R$ 150.000,00	R$ 150.000,00	
16	Renovação do parque de Notebooks	INFRAESTRUTURA DE TI	Atualização do parque tecnológico, a partir do estabelecimento de uma política de atualizações de equipamentos, a fim de Manter o parque computacional em produção atualizado e em garantia.	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 100.000,00	R$ 125.000,00	R$ 125.000,00	
17	Adequação do parque de Servidores	INFRAESTRUTURA DE TI	Adequação contínua do parque de servidores	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 250.000,00	R$ 100.000,00	R$ 300.000,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

CGPOA

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
18	Manutenção da Fitoteca	SERVIÇO DE TI	Contratação de empresa especializada em manutenção das fitotecas adquiridas pelo ITI	Objetivo 7.11	CGPOA	ITI	ESCOLHA:	4	4	4	64	DEMANDAS FUTURAS		R$ 120.000,00	R$ 120.000,00	R$ 120.000,00	
19	Contratação de Empresa Especializada em Métrica de Contagem – FATTO	CONTRATAÇÃO DE TI	Aquisição / manutenção do contrato em vigor de empresa especializada em contagem de ponto de função (Fábrica de Métricas) para auxiliar a fiscalização de contratos de fábrica de software	Objetivo 7.11	CGPOA	ITI	CGPOA	4	4	4	64	DEMANDAS FUTURAS	R$ 21.000,00 *	R$ 18.387,42	R$ 19.306,79	R$ 20.272,13	
20	Solução de impressão	INFRAESTRUTURA DE TI	Elaboração de estudos para o planejamento da contratação	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	3	5	4	60	PRIORIZADO - 2017		R$ 200.000,00	R$ 210.000,00	R$ 220.500,00	
21	Serviço de Administração de Banco De Dados	SERVIÇO DE TI	Contratação do serviço de administração das bases de dados da CODIS	Objetivo 7.12	CGPOA	ITI	ESCOLHA:	4	3	4	48	DEMANDAS FUTURAS		R$ 150.000,00	R$ 157.500,00	R$ 165.375,00	
22	Manutenção do Nobreak do ITI	SERVIÇO DE TI	Contratação de empresa especializada em manutenção dos nobreaks da Autarquia	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	3	4	4	48	DEMANDAS FUTURAS		R$ 50.000,00	R$ 52.500,00	R$ 55.125,00	
23	Solução de inventário de ativos tecnológicos	SERVIÇO DE TI	Estudo e implementação de ferramenta para levantamento, análise, classificação dos ativos computacionais do ITI	Objetivo 7.12	CGPOA	ITI	ESCOLHA:	3	4	3	36	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
24	Contratação de Fábrica de Software - Desenvolvimento	CONTRATAÇÃO DE TI	Contratação de fábrica de software em pontos de função para desenvolvimento de softwares novos para o ITI	Objetivo 7.11	ITI	ITI	ESCOLHA:	3	3	4	36	DEMANDAS FUTURAS		R$ 500.000,00	R$ 600.000,00	R$ 600.000,00	
25	Contratação de Fábrica de Software - Manutenção	CONTRATAÇÃO DE TI	Contratação de fábrica de software em pontos de função para a manutenção dos softwares do ITI	Objetivo 7.11	ITI	ITI	ESCOLHA:	3	3	4	36	DEMANDAS FUTURAS		R$ 500.000,00	R$ 500.000,00	R$ 500.000,00	
26	Solução IDS/IPS	INFRAESTRUTURA DE TI	Melhoria da segurança dos serviços administrados pela CODIS quanto a ataques e tentativa de intrusão	Objetivo 7.13	CGPOA	ITI	ESCOLHA:	4	4	2	32	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
27	Solução de virtualização	INFRAESTRUTURA DE TI	Estudo e aquisição, caso necessário, de solução de virtualização que melhor se adeque às necessidades da CODIS	Objetivo 7.11	CGPOA	CGPOA	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS			R$ 1.000.000,00	R$ 0,00	
28	Ampliação do CFTV	INFRAESTRUTURA DE TI	Aquisição da segunda parte do Circuito Fechado de TV	Objetivo 7.13	CGPOA	ITI	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 100.000,00	R$ 100.000,00	R$ 0,00	
29	Adoção de um Modelo de controle para a Governança de TI	CONTRATAÇÃO DE TI	Ampliação da adoção de orientações contidas no Cobit em processos Da Codis	Objetivo 7.12	CGPOA	CGPOA	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
30	Adoção de um Modelo de melhores práticas Para Gerenciamento de Serviços de TI;	SERVIÇO DE TI	Adoção de orientações do Itil no gerenciamento de serviços oferecidos pela Codis	Objetivo 7.12	CGPOA	CGPOA	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
31	Aplicação de um Modelo de Gerenciamento De Projetos;	CONTRATAÇÃO DE TI	Adoção de práticas de gerenciamento de projetos na Codis	Objetivo 7.12	CGPOA	CGPOA	ESCOLHA:	3	3	3	27	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
32	Manutenção do contrato do SIADS	SERVIÇO DE TI	Prestação de Serviço de Implantação, produção e consultoria do Sistema Integrado de Administração de Serviços – SIADS. Contrato n. 37/2014	Objetivo 7.10	CGPOA	ITI	CGPOA	3	3	3	27	CONTRATADO - 2017	R$ 6.506,40	R$ 21.267,29	R$ 22.330,65	R$ 23.447,19	37/2014
33	Capacitação em normas de Segurança da Informação	PESSOAL DE TI	Gestão de Segurança da Informação (NBR ISO/IEC 27001), Capacitação em Código de Práticas para Gestão da Segurança da Informação Capacitação em Gestão de Riscos	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	3	3	2	18	DEMANDAS FUTURAS		R$ 100.000,00	R$ 100.000,00	R$ 100.000,00	
34	Aquisição de Firewall de Aplicação	INFRAESTRUTURA DE TI	Aquisição de equipamento para aumentar a segurança da informação quanto ao acesso das aplicações Web suportados pela CODIS	Objetivo 7.13	CGPOA	ITI	ESCOLHA:	3	3	2	18	DEMANDAS FUTURAS		R$ 100.000,00	R$ 0,00	R$ 0,00	
35	Adequação do parque de Switches Ethernet	INFRAESTRUTURA DE TI	Adequação contínua o parque de switches ethernet	Objetivo 7.10	CGPOA	CGPOA	ESCOLHA:	3	3	2	18	DEMANDAS FUTURAS		R$ 50.000,00	R$ 50.000,00	R$ 50.000,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
36	Melhoria da arquitetura telefônica do ITI	CONTRATAÇÃO DE TI	Aquisição de equipamentos mais modernos visando a melhoria Dos equipamentos de telefonia utilizados no ITI	Objetivo 7.10	CGPOA	ITI	ESCOLHA:	3	2	2	12	DEMANDAS FUTURAS		R$ 100.000,00	R$ 0,00	R$ 0,00	
37	Adequação do parque de Switches FC	INFRAESTRUTURA DE TI	Adequação contínua o parque de switches FC	Objetivo 7.10	CGPOA	CGPOA	ESCOLHA:	3	2	2	12	DEMANDAS FUTURAS		R$ 360.000,00	R$ 0,00	R$ 180.000,00	
38	Serviço de Mapeamento e Melhoria De Processos	INFRAESTRUTURA DE TI	Contratação de serviço para mapeamento e melhoria de processos	Objetivo 7.12	CGPOA	ITI	ESCOLHA:	3	2	2	12	DEMANDAS FUTURAS		R$ 200.000,00	R$ 100.000,00	R$ 100.000,00	
39	Capacitação em Técnica de Contagem de Ponto de Função – PF	PESSOAL DE TI	Capacitação em PF a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir os objetivos organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	3	2	12	DEMANDAS FUTURAS		R$ 25.000,00	R$ 10.000,00	R$ 0,00	
40	Aquisição de Licença de software de análise De código	SERVIÇO DE TI	Aquisição de Licença de software de análise de código com o objetivo de prover maior segurança aos códigos desenvolvidos	Objetivo 7.11	CGPOA	CGPOA	ESCOLHA:	3	2	2	12	DEMANDAS FUTURAS		R$ 100.000,00	R$ 0,00	R$ 0,00	
41	Capacitação em qualidade de Software	PESSOAL DE TI	Capacitação em CMMI a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir Os objetivos organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	3	12	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
42	Capacitação em COBIT 5	PESSOAL DE TI	Capacitação em Cobit a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir os Objetivos Organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
43	Capacitação em ITIL 2011	PESSOAL DE TI	Capacitação em Itil a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir os Objetivos Organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
44	Capacitação em Balanced Scorecard	PESSOAL DE TI	Capacitação em metodologia de planejamento estratégico	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
45	Capacitação em PMBoK 5	PESSOAL DE TI	Capacitação em PMBoK a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir os Objetivos organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
46	Capacitação em Metodologias de Gestão De Processos (BPM)	PESSOAL DE TI	Capacitação em metodologia de gestão de processos a fim de prover ao pessoal de TI o treinamento apropriado para manter conhecimento, especializações, habilidades e segurança para atingir os objetivos organizacionais.	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 0,00	R$ 0,00	
47	Criação e aprovação do Manual de Gestão De Contratos de TI (MGCTI)	SERVIÇO DE TI	Criação e aprovação de um Manual de Gestão de Contratos de TI, elaborado segundo as normas vigentes, principalmente a IN-4/2010 - SLTI	Objetivo 7.4	CGPOA	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 0,00	R$ 0,00	R$ 0,00	
48	Aquisição de Material Escrito para Capacitação	CONTRATAÇÃO DE TI	Aquisição de normas técnicas e livros	Objetivo 7.4	CGPOA	CGPOA	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 25.000,00	R$ 25.000,00	R$ 25.000,00	
49	Solução de Forense Digital	INFRAESTRUTURA DE TI	Aquisição de solução de perícias forenses, para recuperação e preservação de evidências, para auxiliar no Monitoramento de atividades ilícitas no ambiente interno do Orgão além de auxiliar na recuperação de dados em mídias comprometidas.	Objetivo 7.13	ITI	ITI	ESCOLHA:	2	2	2	8	DEMANDAS FUTURAS		R$ 125.000,00	R$ 0,00	R$ 0,00	
50	Contratação de serviço de consultoria	SERVIÇO DE TI	Contratação de empresa especializada no fornecimento de consultoria para as demandas mais complexas executadas pela CODIS	Objetivo 7.12	CGPOA	CGPOA	ESCOLHA:	2	1	2	4	DEMANDAS FUTURAS		R$ 75.000,00	R$ 75.000,00	R$ 75.000,00	
51	Solução de NOC	INFRAESTRUTURA DE TI	Aquisição de solução de NOC para adequação contínua da infraestrutura de armazenamento, conectividade e do parque de ativos	Objetivo 7.13	CGPOA	CGPOA	ESCOLHA:	1	1	2	2	DEMANDAS FUTURAS		R$ 40.000,00	R$ 40.000,00	R$ 40.000,00	

ITI
Instituto Nacional de Tecnologia da Informação

INVENTÁRIO DE NECESSIDADES – PDTI 2016 2017 2018

ID	NOME DA NECESSIDADE	TIPO DA NECESSIDADE	DESCRIÇÃO DA NECESSIDADE	OBJETIVO DO PE RELACIONADO	ORIGEM	ÁREAS AFETAS	EXECUÇÃO FINANCEIRA	GUT			RESULTADO DA GUT	SITUAÇÃO	EXECUTADO	EXERCÍCIO ATUAL	ESTIMATIVA DOS INVESTIMENTOS		Nº DO CONTRATO
								GRAVIDADE	URGÊNCIA	TENDÊNCIA			2016	2017	2018	2019	
52	Suíte de automação de escritório	SERVIÇO DE TI	O uso intensivo de tecnologia da informação para a edição de textos, elaboração de planilhas e apresentações é inerente às atividades do dia a dia dos colaboradores desta Autarquia. Dessa forma, faz-se necessário uma solução mais robusta que simplifique os processos de trabalho, do ponto de vista administrativo, executados no Instituto, provendo maior celeridade e agilidade na execução deste tipo de atividade.	Objetivo 7.11	CGPOA	ITI	CGPOA	2	2	3	12	PRIORIZADO - 2017		R$ 25.000,00			
53	Aquisição de Licenças Multiponto para Videoconferência	INFRAESTRUTURA DE TI	Tendo em vista o novo direcionamento estratégico estabelecido pela nova gestão do Instituto Nacional de Tecnologia da Informação (ITI), que trouxe, dentre outros, os desafios da massificação do uso do certificado digital para pessoas físicas e o uso do certificado digital imaterial. Dessa forma, a intensificação da agenda de reuniões, seja do Comitê Gestor da ICP-Brasil, seja da COTEC requer uma ferramenta mais efetiva para realização dessas reuniões de forma que a agenda seja mais inclusiva a instituições sediadas fora de Brasília.	Objetivo 7.12	CGPOA	ITI	CGPOA	3	4	4	48	PRIORIZADO - 2017		R$ 8.000,00	R$ 8.000,00	R$ 8.000,00	
54	Consultoria em Pesquisa e Aconselhamento em TIC	SERVIÇO DE TI	Os gestores são constantemente chamados a tomar decisões estratégicas, na maioria das vezes de forma tempestiva, baseado apenas nas suas experiências e conhecimentos. A quantidade de informações disponíveis e ao mesmo tempo dispersas, até mesmo contraditórias, a respeito de características dos componentes e serviços de tecnologia, bem como a dificuldade de monitoramento dos movimentos do mercado, torna necessária a identificação de fontes confiáveis para a obtenção destas e outras informações, bem como, de ferramentas e técnicas para sua compreensão e utilização. Dessa forma, um serviço técnico especializado de pesquisa e aconselhamento em questões tecnológicas permite reduzir o risco de decisão, encurtar o ciclo de decisão e reduzir o risco, bem como aumento da eficiência, produtividade e qualidade dos serviços.	Objetivo 7.12	CGPOA	ITI	CGPOA	3	2	2	12	PRIORIZADO - 2017		R$ 50.000,00	R$ 350.000,00		
													###				

Serviços que foram contratado em 2016 e estão contratados para o exercício de 2017.

* Os valores da Websys e FATTO mencionados não foram executados em 2016, estão em Restos a Pagar.

ANEXO 4

RELAÇÕES DOS SISTEMAS COMPUTACIONAIS, SUAS FUNÇÕES E NECESSIDADES DE NOVAS FUNCIONALIDADES

Anexo 4 - Relação dos Sistemas Computacionais, suas Funções e Necessidades de Novas Funcionalidades

Manutenção de sistemas existentes						
Id	**Nome**	**Descrição**	**Área requisitante**	**Macroprocesso**	**Usuários**	**Tipo de Manutenção Documentação**
1	**SGC**	Gestão do ciclo de vida de certificados digitais emitidos pela Autoridade Certificadora Raiz da ICP-Brasil. Sistema responsável pela gestão de certificados da AC-Raiz e Lista de Certificados Revogados - LCR, ou seja, é utilizado para criar novas Autoridades Certificadoras, bem como assinar os Certificados das Autoridades Certificadoras de 1° Nível. É o software que trabalha com o HSM – Hardware Security Module – Módulo de Segurança Criptográfico que armazena as chaves privadas da AC-Raiz para as assinaturas de Certificados e LCRs – Listas de Certificados Revogados.	DINFRA	Gestão da AC Raiz da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software (TDC UFSC) como para o hardware (Kryptus).
1.1	**YWAPA**	É o software de gestão de certificados da AC – Raiz.	DINFRA	Gestão da AC Raiz da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. TDC UFSC
1.2	**YWYRA**	É software de gestão de certificados para as ACs de 1° nível que não emitem certificados para usuários finais.	DINFRA	Gestão da AC Raiz da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. TDC UFSC
1.3 4	**HAWA**	É software de gerenciamento de certificados para ACs que emitem certificados para usuários finais.	DINFRA	Gestão da AC Raiz da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. TDC UFSC
2	**SAS BRY**	O Carimbo do Tempo é um selo que atesta a data e a hora exata em que um documento eletrônico recebeu a assinatura digital. Desta forma, garante a veracidade das informações e que o documento não sofreu adulteração no intervalo de tempo entre a assinatura e a consulta ao documento. O Carimbo do Tempo somente tem validade legal incontestável se emitido por uma Autoridade de Carimbo do Tempo (ACT) credenciada pelo ITI	DINFRA	Carimbo do Tempo da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. BRY

		- Instituto da Tecnologia da Informação. Sistema de Auditoria e Sincronismo de Tempo – O sistema audita as carimbadoras de tempo e emite alvarás para seu funcionamento (autorizações para emitir carimbo de tempo). A BRY e THALES são duas tecnologias proprietárias que executam a mesma função, porém como o mercado pode utilizar uma como outra e elas não são interoperáveis, o ITI disponibilizas as duas opções de forma a atender a todas as demandas				
3	**TSMC THALES**	O Carimbo do Tempo é um selo que atesta a data e a hora exata em que um documento eletrônico recebeu a assinatura digital. Desta forma, garante a veracidade das informações e que o documento não sofreu adulteração no intervalo de tempo entre a assinatura e a consulta ao documento. O Carimbo do Tempo somente tem validade legal incontestável se emitido por uma Autoridade de Carimbo do Tempo (ACT) credenciada pelo ITI - Instituto da Tecnologia da Informação. O sistema audita as carimbadoras de tempo e emite alvarás para seu funcionamento (autorizações para emitir carimbo de tempo). A BRY e THALES são duas tecnologias proprietárias que executam a mesma função, porém como o mercado pode utilizar uma como outra e elas não são interoperáveis, o ITI disponibilizas as duas opções de forma a atender a todas as demandas	DINFRA	Carimbo do Tempo da ICP-Brasil	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. THALES
4	**Gerador de Políticas de Assinatura da ICP-Brasil**	Gestão de políticas de assinatura digital, conforme normativos vigentes na ICP-Brasil (DOC-ICP-15). É o software que gera e assina as políticas de assinatura e as disponibiliza para o mercado	ITI	*Gestão de Políticas de Assinatura da ICP-Brasil*	ICP-Brasil	Exige contrato de manutenção preventiva, corretiva e evolutiva tanto para o software como para o hardware. TDC UFSC
5	**Validador**	Ferramenta de validação e verificação de certificados e LCRs emitidos no âmbito da ICP-Brasil. Permite verificar a conformidade de certificados e LCRs com base nas políticas de certificação aprovadas pela ICP-Brasil. Permite extrair o conteúdo desses artefatos. Codificado em Java com banco de Dados PostgreSQL.	DAFN	Auditoria	DAFN	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS

		Utiliza biblioteca criptográfica EVO-SDK.				
6	**Auditoria**	Base de informações de controles de auditoria realizadas pelo ITI, empresas de auditoria independentes e auditorias internas da ICP-Brasil Codificado em Java com banco de Dados PostgreSQL. Utiliza biblioteca criptográfica EVO-SDK. Faz integração com os sistemas Cadastros, Fiscalização, Credenciamento e RiskManager Algumas informações são públicas e poderiam ser disponibilizada para a sociedade.	DAFN	Gestão do ITI	DAFN Público	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS
7	**Credenciamento**	Ferramenta de automação do processo de credenciamento das entidades da ICP-Brasil. Possibilita a realização de ciclo completo de credenciamento com interação do ITI e das entidades credenciadas e em credenciamento de forma automatizada. Codificado em Java com banco de Dados PostgreSQL. Utiliza biblioteca criptográfica EVO-SDK. Mantém informações cadastrais e possibilita o credenciamento Faz integração com Cadastros, Fiscalização e Auditoria. As informações são públicas e de acesso a toda a sociedade.	DAFN	Gestão do ITI	ITI Entidades da ICP-Brasil Público	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS
8	**Cadastro**	Base de informações de entidades credenciadas/em credenciamento na ICP-Brasil. Mantém informações cadastrais das entidades participantes da ICP-Brasil. Codificado em Java com banco de Dados PostgreSQL. Utiliza biblioteca criptográfica EVO-SDK. Algumas informações podem ser disponibilizadas para o público.	DAFN	Gestão do ITI	DAFN Público	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS
9	**Fiscalização**	Gerenciamento dos trabalhos de fiscalização nas entidades integrantes da ICP-Brasil. Desenvolvida em Java. Compartilha a base de dados do Cadastro. Utiliza biblioteca criptográfica EVO-SDK.	DAFN	Gestão do ITI	ITI Entidades ICP-Brasil	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS
10	**Monitor**	Faz o monitoramento automático do repositório das AC's de forma remota possibilitando o registro de falhas e emissão de alertas. Codificado em Java com banco de Dados PostgreSQL. Utiliza biblioteca criptográfica EVO-SDK.	DAFN	Auditoria e Fiscalização	DAFN	Exige contrato de manutenção corretiva, adaptativa e evolutiva. WEBSYS
11	**Monitoramento de Certificado ***	Base de informações de certificados emitidos pelas	DAFN	Gestão do ITI	ITI	Exige contrato de manutenção evolutiva e

		entidades na ICP-Brasil, possui também base de Fraudes/tentativas de fraude na emissão dos certificados digitais. Sistema Anti-Fraude da ICP-Brasil - SAF (Lista Negativa e Comunicado de Fraude): Criado para aprimorar os processos de emissão do certificado digital, e respectivas fiscalizações, principalmente combatendo o uso de identidade falsificada pelo requerente de um certificado digital. O primeiro módulo desse sistema é a Lista Negativa que contêm as informações de todo o processo do requerente que falsificou, ou tentou falsificar, a emissão de um certificado digital. Tem a função de estabelecer uma comunicação *on-line* entre os servidores das Autoridades Certificadoras e do ITI, no intuito de comunicar e disponibilizar as informações de fraudes, ou tentativas, por uso de identidade falsa para todo o sistema da ICP-Brasil, possibilitando um melhor gerenciamento das fiscalizações por parte do ITI e atualizações dessas informações para toda cadeia de Autoridades Certificadoras e Autoridades de Registro.				agregação de novas funcionalidades. Sistema Anti-Fraude da ICP-Brasil - SAF (Lista Positiva): A Lista Positiva é a informação verdadeira dos requerentes de um certificado digital. Faz-se necessário visto que mais de noventa por cento das fraudes na ICP-Brasil são por uso irregular de identidade de pessoas e/ou empresas que de fato existem e que já possuem um certificado digital. Com isso, existe uma mitigação da emissão irregular de um certificado digital, visto que teremos disponível as informações verdadeiras atreladas ao titular de fato do documento de identificação. As normas para tal Sistema, Lista Positiva, já estão escritas, também no que tange a obtenção dos *hardwares* e *softwares* para construção dessa Lista Positiva, mas ainda está pendente a aprovação por parte do Comitê Gestor da ICP-Brasil e das entidades participes da ICP-Brasil. WEBSYS
12	**Verificador de Conformidade PBAD**	Sistema disponivel no portal do ITI para verificações de documentos assinados no Padrão Brasileiro de Assinatura Digital (PBAD).	ITI	Gestão de Assinaturas Digital	ICP Brasil e Sociedade Geral	Manutenção evolutiva à medida que ocorrer alterações nos documentos do PBAD. TDC UFSC
13	**Assinador Digital**	Sistema de assinatura digital do PBAD conforme DOC-ICP-15.	ITI	Gestão de Assinaturas Digital	ITI e Sociedade Geral	Manutenção evolutiva à medida que ocorrer alterações nos documentos do PBAD. TDC UFSC
14	**Plug-in PAdES ICP-Brasil**	Software que implementa verificação de assinatura digital para aplicativo leitor de arquivos PDF no padrão PAdES ICP-Brasil.	ITI	Verficação de Assinaturas Digital padrão ICP-Brasil	ITI e Sociedade Geral	Requer manutenção corretiva e evolutiva. TED UnB.

*Projeto de conversão para tecnologia Java JBPM com utilização da base de dados corporativa e controle de acesso a usuários externos com uso de certificado digital ICP - BRASIL.

ANEXO 5

GLOSSÁRIO

GLOSSÁRIO ICP-BRASIL

Versão 1.5

27.03.2018

PALAVRA CHAVE	DESCRIÇÃO
ABNT (Associação Brasileira de Normas Técnicas)	Fundada em 1940, é o órgão responsável pela normalização técnica no país, fornecendo a base necessária ao desenvolvimento tecnológico brasileiro.
Aceitação do Certificado Digital	Demonstração da concordância de uma pessoa física ou jurídica quanto à correção e adequação do conteúdo e de todo o processo de emissão de um certificado digital, feita pelo indivíduo ou entidade que o solicitou. O certificado é considerado aceito a partir de sua primeira utilização, ou após haver decorrido o prazo preestipulado para sua rejeição. A aceitação do certificado será declarada pelo titular.
Acesso	Estabelecimento de conexão entre um indivíduo ou entidade e um sistema de comunicação ou de informações. A partir do Acesso podem ocorrer a transferência de dados e a ativação de processos computacionais.
Acesso Físico	Habilidade de obter acesso a um ambiente físico. Os sistemas de controle de Acesso Físico possibilitam a integração de funcionalidades, com leitores biométricos, alarmes de incêndio, emissão de crachás para visitantes, etc.
Acesso lógico	O Controle de Acesso Lógico permite que os sistemas de Tecnologia da Informação verifiquem a identidade dos usuários que tentam utilizar seus serviços. Como exemplo mais comum, temos o *logon* de um usuário em um computador.
Acesso Remoto	Habilidade de obter acesso a um computador ou uma rede a distância. As conexões *dial-up, wireless*, DSL são exemplos de possibilidades de Acesso Remoto.
AES (Advanced Encryption Standard)	O Padrão de Cifração Avançada (AES) é uma cifra de bloco adotada como padrão de cifração pelo governo dos Estados Unidos. O AES é um dos algoritmos mais populares usados na criptografia de chave simétrica. AES tem um tamanho de bloco fixo de 128 bits e uma chave com tamanho de 128, 192 ou 256 bits.
Agente de Registro	Responsável pela execução das atividades inerentes à AR. É a pessoa que realiza a autenticação da identidade de um individuo ou de uma organização e validação das solicitações de emissão e revogação de certificados nas Autoridades de Registro.
Agentes Causadores de Eventos	É uma pessoa, organização, dispositivo ou aplicação que causa um evento registrado pelo conjunto de sistemas de auditoria.

PALAVRA CHAVE	DESCRIÇÃO
Algoritmo	Série de etapas utilizadas para completar uma tarefa, procedimento ou fórmula na solução de um problema. Usado como "chaves" para criptografia de dados.
Algoritmo Assimétrico	É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave.
Algoritmo Criptográfico	Processo matemático especificamente definido para cifrar e decifrar mensagens e informações, normalmente com a utilização de chaves.
Algoritmo Simétrico	Algoritmo de criptografia que usa somente uma chave, tanto para cifrar como para decifrar. Esta chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta.
Alvará	Documento eletrônico assinado digitalmente pela Entidade Auditora para uma Autoridade de Carimbo do Tempo, através de um sistema de auditoria e sincronismo. Consiste em um certificado de atributo no qual estarão expressos os dados referentes ao sincronismo e o parecer do auditor sobre a exatidão do relógio da entidade auditada.
Ambiente Físico	Ambiente composto pelos ativos físicos permanentes das entidades integrantes da ICP-Brasil.
Ambiente Lógico	Ambiente composto pelos ativos de informação das entidades integrantes da ICP-Brasil.
Análise de Risco	Identificação e avaliação dos riscos (vulnerabilidades e impactos) a que os ativos da informação estão sujeitos.
Aplicações do Certificado	Os certificados da ICP-Brasil são utilizados, de acordo com o seu tipo, em aplicações como: i. **Tipo A**: confirmação da identidade na *web*, correio eletrônico, transações *on-line,* redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações. ii. **tipo S**: cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Applet	Aplicativo executado no contexto de outro programa.
Arquivamento de	Armazenamento da chave privada para seu uso futuro, após o período de

PALAVRA CHAVE	DESCRIÇÃO
Chave privada	validade do certificado correspondente. Só se aplica a chaves privadas de certificados de sigilo. As chaves privadas de assinatura digital só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
Arquivamento de chave Pública	Armazenamento da chave pública, por um período mínimo de 30 anos, para uso futuro, após o período de validade do certificado correspondente com o objetivo de verificar as assinaturas geradas durante o prazo de validade dos respectivos certificados. Só se aplica a chaves públicas de certificados de assinatura. As chaves públicas de sigilo só poderão ser utilizadas durante o período de validade dos respectivos certificados, sendo portanto proibido seu armazenamento.
Arquivo dedicado *(Dedicated File – DF)*	Corresponde a um arquivo que contém informações de controle sobre outros arquivos e, opcionalmente, sobre a memória disponível para alocação. Também pode corresponder a um diretório que permite que outros arquivos e/ou diretórios (EF e DF) possam estar contidos, vinculados ou agrupados [ISO/IEC 7816-4].
Arquivo elementar *(Elementary File – EF)*	Corresponde a um conjunto de unidades de dados ou registros que compartilham o mesmo identificador de arquivo. Por exemplo, dados necessários para uma aplicação são armazenados em EF. Um EF não pode ser "pai" (pertencer a um nível hierárquico superior na árvore de arquivos e diretórios) de outro arquivo [ISO/IEC 7816-4].
Arquivo "Pai"	Corresponde ao arquivo dedicado (DF) imediatamente precedente a um dado arquivo dentro da hierarquia [ISO/IEC 7816-4].
ASN.1 (Abstract Syntax Notation 1)	Notação formal usada para descrever os dados transmitidos por protocolos de telecomunicações, não obstante a representação física destes dados, o que quer que a aplicação faça, seja complexo ou muito simples.
Assinatura Digital	Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um *e-mail* ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem

PALAVRA CHAVE	DESCRIÇÃO
	do dado é feita com a chave pública do remetente.
Ataque	i. Ato de tentar desviar dos controles de segurança de um programa, sistema ou rede de computadores. Um ataque pode ser ativo, tendo por resultado a alteração dos dados; ou passivo, tendo por resultado a liberação dos dados. ii. Tentativa de criptoanálise. O fato de um ataque estar acontecendo não significa necessariamente que ele terá sucesso. O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia de contramedidas existentes.
Ativação de Chave	Método pelo qual a chave criptográfica fica pronta para exercer suas funções. A ativação da chave se dá por meio de um módulo criptográfico, após a identificação dos operadores responsáveis. A identificação pode ocorrer através de uma senha ou outro dispositivo de controle de acesso como um *token, smart card*, biometria.
Ativo de Informação	Patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos de uma organização.
Ativo de Processamento	Patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos
Atribuição de Chaves *(Key Establishment)*	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada a parceiros legítimos. A atribuição de chaves pode ser realizada por um processo automático (protocolo de negociação de chaves ou protocolo de transporte de chaves), método manual ou uma combinação dos anteriores.
Auditor	Profissional que realiza a avaliação dos controles e processos das entidades auditadas. Deve ser idôneo, dotado de capacidades e conhecimentos técnicos específicos e realizar o seu trabalho com observância de princípios, métodos e técnicas geralmente aceitos. Não deve possuir nenhum dos impedimentos ou suspeições estabelecidos nas normas da ICP-Brasil e no Código de Processo Civil.
Auditor Independente	Auditor que não está vinculado aos quadros do ITI nem da entidade auditada. Trabalha para uma empresa de auditoria independente.
Auditoria	Procedimento utilizado para verificar se todos os controles, equipamentos e dispositivos estão preparados e são adequados às regras, normas, objetivos e funções. Inclui o registro e análise de todas as

PALAVRA CHAVE	DESCRIÇÃO
	atividades importantes para detectar vulnerabilidades, determinar se houve violação ou abusos em um sistema de informações com vista a possibilitar ao auditor formar uma opinião e emitir um parecer sobre a matéria analisada.
Auditoria de Conformidade	Avaliação da adequação dos processos, procedimentos e atividades das unidades auditadas com a legislação e os regulamentos aplicáveis. Verificam-se todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Auditoria Independente	Auditoria realizada por Empresa de Auditoria Especializada e Independente.
Auditoria Operacional	Auditoria de conformidade realizada após o processo de credenciamento. Realizada anualmente ou a qualquer momento, se houver suspeitas de irregularidades.
Auditoria Pré-operacional	Auditoria de conformidade realizada antes do processo de credenciamento.
Autenticação	Processo de confirmação da identidade de uma pessoa física (Autenticação de um Individuo) ou jurídica (Autenticação da Identidade de uma Organização) através das documentações apresentadas pelo solicitante e da confirmação dos dados da solicitação. Executado por Agentes de Registro, como parte do processo de aprovação de uma solicitação de certificado digital.
Autenticação do Agente de Registro	Verificação da identidade de um Agente de Registro, em um sistema computadorizado, como um pré-requisito para permitir o acesso aos recursos de um sistema. Na ICP-Brasil a autenticação do Agente deve se dar com o uso de certificado que tenha requisito de segurança, no mínimo, equivalente ao de um certificado A3.
Autenticação e Sincronização de Relógio (ASR)	Atividade periodicamente realizada pela EAT que resulta na habilitação ou não de um SCT para operar sincronizado com a hora UTC. Essas operações devem ser efetuadas por intermédio de um conjunto de protocolos que garantam que o resultado final seja isento de fraudes.
Autenticidade	Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção.
Autoassinatura digital	Assinatura feita usando a chave privada correspondente à chave pública

PALAVRA CHAVE	DESCRIÇÃO
	associada ao certificado digital.
Autoteste	Estratégia proposta inicialmente para ser utilizada em classes de sistemas orientados a objetos. Nesta estratégia, é incorporada uma especificação de testes à classe, além do acréscimo de funções BIT (do inglês *Built-in Test*) que criam capacidades de observação e controle do estado da classe. A ideia principal é a incorporação ao componente da capacidade de gerar casos de testes automaticamente, ou da inclusão de casos de teste já prontos. Esses casos de teste podem ser executados pelo cliente ou pelo próprio componente.
Autoridade Certificadora (AC)	Entidade que emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Além disso, emite e publica LCR. Na estrutura de carimbo de tempo da ICP-Brasil, emite os certificados digitais usados nos equipamentos e sistemas das ACTs e da EAT.
Autoridade Certificadora Raiz (AC Raiz)	Entidade que credencia, audita e fiscaliza as demais entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das ACs imediatamente abaixo dela. É também a Entidade de Auditoria do tempo da Rede de Carimbo do Tempo da ICP-Brasil.
Autoridade de Carimbo de Tempo (ACT)	Entidade na qual os usuários de serviços de carimbo do tempo – subscritores e terceiras partes, confiam para emitir carimbos do tempo. A ACT tem a responsabilidade geral pelo fornecimento do carimbo do tempo. É responsável pela operação de um ou mais SCT, conectados à Rede de Carimbo do Tempo da ICP-Brasil.
Autoridade de Registro (AR)	Entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.
Autoridade Gestora de Políticas da ICP-Brasil	Vide Comitê Gestor da ICP-Brasil
Autorização	Concessão de direito ou permissão que inclui a capacidade de acessar informações e recursos específicos em um sistema computacional ou permissão de acesso a ambientes físicos.
Autorização de Auditoria Independente	Constitui ato declaratório do Diretor de Auditoria, Fiscalização e Normalização do ITI que permite ao Auditor Independente prestar serviços de auditoria, no âmbito da ICP-Brasil, em conformidade com as

PALAVRA CHAVE	DESCRIÇÃO
	normas estabelecidas por este Comitê Gestor.
Avaliação de Conformidade	Conjunto de ensaios com o objetivo de verificar se os padrões e especificações técnicas mínimas aplicáveis a um determinado sistema ou equipamento de certificação digital estão atendidos.
Backup	Vide Cópia de Segurança
Banco de dados	Basicamente é um conjunto de informações relacionadas que são reunidas de forma organizada e categorizada, assim como os "arquivos tradicionais em forma de fichas", porém armazenados em meio magnético (disco de computadores) e que são "Gerenciados" por "Sistemas Especializados", ou, os chamados "Sistemas Gerenciadores de Banco de Dados" (ex: *MYSQL, SQL Server, Oracle, DB2, IMS/DLI, ADABAS*, etc.), que permitem armazenagem, atualização e recuperação dessas informações de forma eficiente (fácil, rápida e precisa) independente do volume.
BASE64	Método para codificação de dados para transferência na Internet (*Content Transfer Enconding*).
BER (Basic Encoding Rules)	Regras para codificação de objetos ASN.1 em uma sequência de *bytes*.
Biometria	Ciência que utiliza propriedades físicas e biológicas únicas e exclusivas para identificar indivíduos. São exemplos de identificação biométrica as impressões digitais, o escaneamento de retina e o reconhecimento de voz.
Binary digit (Bit)	Menor unidade de informação possível dentro de um computador. Pode assumir os valores de 0 ou 1.
Bloco	Sequência de bits de comprimento fixo.
Buffer	Região de memória temporária utilizada para escrita e leitura de dados. Os dados podem ser originados de dispositivos (ou processos) externos ou internos ao sistema. Os *buffers* podem ser implementados em software (mais usado) ou hardware. Normalmente são utilizados quando existe uma diferença entre a taxa em que os dados são recebidos e a taxa em que eles podem ser processados, ou no caso em que essas taxas são variáveis.
***Bureau International des Poids et Mesures* (BIPM)**	Organização central do Sistema Internacional de Metrologia localizada na França e responsável pela geração do UTC.
Cache	Bloco de memória para o armazenamento temporário de dados que

PALAVRA CHAVE	DESCRIÇÃO
	possuem uma grande probabilidade de serem utilizados novamente.
Cadastro de Agente de Registro (CAR)	Conjunto formal de dados, gerido pelo ITI, para centralização das informações cadastrais dos agentes de registro que atuam no âmbito da ICP-Brasil.
Cadastro de Auditoria Independente	Registro cadastral oficial do ITI das empresas de auditoria especializada e independente. Para almejar o cadastro a empresa deverá apresentar ao ITI rol de documentos previstos na resolução 44 do CG da ICP-Brasil. O cadastro terá validade de 5 anos sendo possível renovações.
Cadastro Nacional de Nomenclaturas (CNN)	Banco de dados público, gerido pela Procuradoria Federal Especializada/ ITI, que tem por finalidade evitar a ocorrência de identidade ou semelhança entre as nomenclaturas adotadas pelas entidades integrantes da ICP-Brasil.
Cadeia de AC	Interligações hierárquicas existentes entre as diversas Autoridades Certificadoras participantes da ICP-Brasil.
Cadeia de Certificação	Série hierárquica de certificados assinados por sucessivas autoridades certificadoras.
Carimbo de Tempo (CT)	Documento eletrônico emitido pela ACT, que serve como evidência de que uma informação digital existia numa determinada data e hora passada.
Cartão Inteligente	Vide *Smart Card*
Cavalo-de-Tróia	Programa no qual um código malicioso ou prejudicial está contido dentro de uma programação ou dados aparentemente inofensivos de modo a poder obter o controle e causar danos.
CBC (Cipher Block Chaining)	Modo de operação de uma cifra de bloco (ver cifra de bloco), em que o texto plano primeiro é submetido a uma operação binária de XOR com o criptograma resultante do bloco anterior. Algum valor conhecido é usado para o primeiro bloco (normalmente chamado de vetor de inicialização**,** esse valor deve ser único para cada mensagem, mas não precisa ser secreto – pode ser enviado junto com o criptograma, para permitir a decifração). O resultado é então cifrado usando a chave simétrica. Assim, blocos de entrada idênticos em texto claro produzirão criptogramas diferentes.
Certificação de Data e Hora	Vide *Time-stamping*

PALAVRA CHAVE	DESCRIÇÃO
Certificação Digital	Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.
Certificado de Atributo	Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.
Certificado Autoassinado	Certificado assinado com a chave privada da própria entidade que o gerou. O único certificado autoassinado da ICP-Brasil é o da Autoridade Certificadora Raiz.
Certificado de Calibração	Documento emitido pelo Observatório Nacional atestando que o equipamento usado para emitir carimbos de tempo (SCT) está dentro dos padrões de sincronismo esperados e está apto a entrar em funcionamento.
Certificado de Assinatura Digital (A1, A2, A3 e A4)	São os certificados usados para confirmação da identidade na *web*, correio eletrônico, transações *on-line,* redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações.
Certificado de Especificações	Documento com as descrições dos requisitos atendidos pelo SCT, no qual o seu fabricante declara responsabilidade sobre estas características. Cada certificado é restrito a um SCT.
Certificado de Sigilo (S1, S2, S3 e S4)	Certificados usados para cifração de documentos, bases de dados, mensagens e outras informações eletrônicas.
Certificado digital	Conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.
Certificado do Tipo A1 e S1	Certificado em que a geração das chaves criptográficas é feita por software e seu armazenamento pode ser feito em hardware ou repositório protegido por senha, cifrado por *software.* Sua validade máxima é de um ano, sendo a frequência de publicação da LCR no máximo de 48 horas e o prazo máximo admitido para conclusão do processo de revogação de

PALAVRA CHAVE	DESCRIÇÃO
	72 horas.
Certificado do Tipo A2 e S2	Certificado em que a geração das chaves criptográficas é feita em software e as mesmas são armazenadas em Cartão Inteligente ou *Token,* ambos sem capacidade de geração de chave e protegidos por senha. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de dois anos, sendo a frequência de publicação da LCR no máximo de 36 horas e o prazo máximo admitido para conclusão do processo de revogação de 54 horas.
Certificado do Tipo A3 e S3	Certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 1024 bits. A validade máxima do certificado é de três anos, sendo a freqüência de publicação da LCR no máximo de 24 horas e o prazo máximo admitido para conclusão do processo de revogação de 36 horas.
Certificado do Tipo A4 e S4	Certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *Token*, ambos com capacidade de geração de chaves e protegidos por senha, ou *hardware* criptográfico aprovado pela ICP-Brasil. As chaves criptográficas têm no mínimo 2048 bits. A validade máxima do certificado é de três anos, sendo a frequência de publicação da LCR no máximo de 12 horas e o prazo máximo admitido para conclusão do processo de revogação de 18 horas.
Certificado Expirado	Certificado cuja data de validade foi ultrapassada.
Certificado Válido	Certificado dentro do prazo de validade, que não tenda sido revogado e que seja possível validar toda a cadeia do certificado até uma AC Raiz.
CFB (Ciphertext Feedback)	Modo de operação para uma cifra de bloco (ver Cifra de Bloco), no qual a saída do sistema é retroalimentada no mecanismo. Depois que cada bloco é cifrado, parte dele sofre um deslocamento em um registrador. O conteúdo desse registrador é cifrado usando a chave do usuário e a saída sofre uma nova operação binária de XOR com os dados de entrada, para produzir o criptograma. Nesse modo, podemos trabalhar com blocos de mensagens menores do que o tamanho nativo do algoritmo. Dependendo do sistema externo onde está inserido o sistema criptográfico, isso pode trazer vantagens, pois evita a utilização de *buffers* para armazenar temporariamente

PALAVRA CHAVE	DESCRIÇÃO
	elementos da mensagem até completar o tamanho de bloco do algoritmo. Efetivamente, o que se obterá é uma conversão do algoritmo, que opera em forma nativa como cifrador de blocos, em um sistema de cifração sequencial. Esse método é auto-sincronizável e permite que o usuário decifre apenas uma parte de uma grande base de dados, se começar a partir de uma distância fixa dos dados desejados.
Chave Criptográfica	Valor numérico ou código usado com um algoritmo criptográfico para transformar, validar, autenticar, cifrar e decifrar dados.
Chave Criptográfica em Texto Claro	Representa uma chave criptográfica não cifrada.
Chave Criptográfica Secreta	Vide Chave Privada e Chave Simétrica
Chave de Sessão	Chave para sistemas criptográficos simétricos. Utilizada pela duração de uma mensagem ou sessão de comunicação. O protocolo SSL (*Secure Sockets Layer)* utiliza as chaves de sessão para manter a segurança das comunicações via internet.
Chave Privada	Chave secreta do par de chaves criptográficas (a outra é uma chave pública) em um sistema de criptografia assimétrica. É mantida secreta pelo seu dono (detentor de um certificado digital) e usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente.
Chave Pública	Chave mantida pública (a outra é uma chave privada) em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente. Dependendo do algoritmo, a chave pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a chave privada correspondente.
Chave Simétrica	Chave criptográfica gerada por um algoritmo simétrico (Ver Algoritmo Simétrico).
Chaves Assimétricas	Chaves criptográficas geradas por um algoritmo assimétrico (Ver Algoritmo Assimétrico).
Ciclo de Vida do Certificado	Período de tempo que se inicia com a solicitação do certificado e termina com sua expiração ou revogação.
Cifra	Algoritmo criptográfico utilizado para prover confidencialidade à informação.

PALAVRA CHAVE	DESCRIÇÃO
Cifra de Bloco	Algoritmo criptográfico simétrico, no qual a mensagem é dividida em blocos e cada bloco é cifrado separadamente.
Cifrar	i. Processo de transformação de dados ou informação para uma forma ininteligível usando um algoritmo criptográfico e uma chave criptográfica. Os dados não podem ser recuperados sem usar o processo inverso de decifração. ii. Processo de conversação de dados em "código ilegível" de forma a impedir que pessoas não autorizadas tenham acesso à informação.
Classificação da Informação	Ato ou efeito de analisar e identificar o conteúdo de documentos, atribuindo um grau de sigilo que define as condições de acesso aos mesmos, conforme normas e legislação em vigor.
CMM-SEI (Capability Maturity Model do Software Engineering Institute)	Modelo para avaliação da maturidade dos processos de software de uma organização e para identificação das práticas-chave que são requeridas para aumentar a maturidade desses processos. O CMM prevê cinco níveis de maturidade: inicial, repetível, definido, gerenciado e otimizado. O modelo foi proposto por Watts S. Humphrey, a partir das propostas de Philip B. Crosby, e vem sendo aperfeiçoado pelo *Software Engineering Institute* - SEI da Carnegie Mellon University.
CMPV (Cryptographic Module Validation Program)	Programa de testes para módulos criptográficos criado pelo *NIST (National Institute of Standards and Technology*, do governo dos Estados Unidos, e pelo CSE (*Communications Security Establishment*) do governo do Canadá, em 1995. Utiliza-se de laboratórios independentes credenciados. Fabricantes interessados nos testes de validação podem selecionar qualquer um dos laboratórios credenciados. Para as validações, são utilizados os requisitos definidos no padrão FIPS 140-2.
CMS (Cryptographic Message Syntax)	Padrão do IETF definido na RFC 3852. Esta sintaxe é baseada nas especificações do PKCS#7, que por sua vez se baseia no Privacy-Enhanced Mail - PEM. Pode ser usado para assinatura digital, hash, autenticação ou cifração de qualquer formato de dado digital.
CN (Common Name)	Atributo especificado dentro do campo Assunto - Nome Distinto (*Distinguished Name*) - de um certificado. Por exemplo, para certificados de servidor o nome do *"host"* DNS do site a ser certificado; para um Certificado de Assinatura de Software, o nome comum é o nome da organização e em certificados de assinante, o nome comum é normalmente composto pelo prenome e sobrenome do titular.
Coassinatura	Assinatura gerada de maneira independente das outras assinaturas.

PALAVRA CHAVE	DESCRIÇÃO
Código de Autenticação	Verificador criptográfico de integridade e autenticidade que é comumente referenciado como MAC (*Message Authentication Code*).
Comissão Técnica Executiva (COTEC)	Comissão técnica que presta suporte técnico e assistência ao Comitê Gestor da ICP-Brasil, sendo responsável por manifestar previamente sobre as matérias apreciadas e decididas pelo comitê Gestor.
Comitê Gestor da ICP-Brasil	Entidade responsável pela implantação da ICP-Brasil. Estabelece políticas, critérios e normas de funcionamento que devem ser seguidas pelas entidades integrantes da ICP-Brasil. Audita e fiscaliza a AC-Raiz.
Commom Criteria (CC)	Padrão internacional (ISO/IEC 15408) para a segurança do computador. CC fornece a garantia que o processo da especificação, da execução e da avaliação de um produto de segurança do computador foi conduzido de modo rigoroso e padronizado.
Compensação (*Offset*)	Correção necessária no relógio local para fazer com que indique o mesmo tempo indicado pelo relógio de referência.
Comprometimento	Violação concreta ou suspeita de violação de uma política de segurança de um sistema, onde possa ter ocorrido divulgação não autorizada ou perda do controle sobre informações sigilosas.
Confiança	Suposição de que uma entidade se comportará substancialmente como esperado no desempenho de uma função específica.
Confidencial	Tipo de classificação de informação, que se for divulgada ou usada sem autorização, trará sérios prejuízos para uma organização.
Confidencialidade	Propriedade de certos dados ou informações que não podem ser disponibilizadas ou divulgadas sem autorização para pessoas, entidades ou processos. Assegurar a confidencialidade de documentos é assegurar que apenas pessoas autorizadas tenham acesso à informação.
Confirmação da Identidade	Vide Autenticação da Identidade
Consulta *On-line* de Situação do Certificado	Vide OCSP
Conta	Permissão para acesso a um serviço. A permissão é obtida após o registro de dados específicos do usuário, no servidor, que definem o ambiente de trabalho desse usuário. O registro pode incluir configurações de tela, configurações de aplicativos e conexões de rede. O que o usuário vê na tela, além de quais arquivos, aplicativos e diretórios ele tem acesso é

PALAVRA CHAVE	DESCRIÇÃO
	determinado pela maneira com que foi configurada a conta do usuário.
Contexto Seguro de Execução	Estrutura de dados existente durante a execução da biblioteca criptográfica onde as chaves criptográficas estão protegidas contra divulgação, modificação e substituição não autorizada.
Contingência	Situação excepcional decorrente de um desastre.
Contra-assinatura	Contra-assinatura (*countersign*) é aquela realizada sobre uma assinatura já existente. Na especificação CMS a contra-assinatura é adicionada na forma de um atributo não autenticado (*countersignature attribute*) no bloco de informações (*signerInfo)* relacionado à assinatura já existente.
Controle "n de m"	Forma de controle múltiplo onde "n" pessoas de um grupo de "m", são requeridas para utilização de uma chave privada.
Controle de Acesso	i. Conjunto de componentes dedicados a proteger a rede, aplicações *Web* e instalações físicas de uma AC contra o acesso não autorizado, permitindo que somente organizações ou indivíduos previamente identificados e autorizados possam utilizá-las. ii. Restrições ao acesso às informações de um sistema, exercidas pela gerência de segurança da entidade detentora daquele sistema.
Controles	i. Procedimentos usados para controlar o sistema de tal maneira que ele esteja de acordo com critérios especificados. ii. Qualquer ação, procedimento, técnica ou qualquer outra medida que reduza a vulnerabilidade de uma ameaça a um sistema.
Cópia de Segurança	Cópias feitas de um arquivo ou de um documento que deverão ser guardadas sob condições especiais para a preservação de sua integridade no que diz respeito tanto à forma quanto ao conteúdo, de maneira a permitir o resgate de programas ou informações importantes em caso de falha ou perda dos originais.
Credenciamento	Processo em que o ITI avalia e aprova os documentos legais, técnicos, as práticas e os procedimentos das entidades que desejam ingressar na ICP-Brasil. Aplica-se a Autoridades Certificadoras, Autoridades de Registro e Prestadores de Serviços de Suporte. Quando aprovados, os credenciamentos são publicados no Diário Oficial da União.
CryptoAPI	*Cryptographic Application Programming Interface* (também conhecida como *CryptoAPI, Microsoft Cryptography API*, ou simplesmente *CAPI*) é uma interface de programação para aplicações incluída com o sistema operacional *Microsoft Windows* que provê serviços para habilitar desenvolvedores para aplicações de segurança baseadas em *Windows*

PALAVRA CHAVE	DESCRIÇÃO
	usando criptografia. É um conjunto de bibliotecas dinamicamente ligadas que provê um nível de abstração que isola programadores do código usado para cifrar dados.
Criptografar	Ver Cifrar
Criptografia	i. Disciplina de criptologia que trata dos princípios, dos meios e dos métodos de transformação de documentos com o objetivo de mascarar seu conteúdo, impedir modificações, uso não autorizado e dar segurança à confidência e autenticação de dados. ii. Ciência que estuda os princípios, meios e métodos para tornar ininteligíveis as informações, através de um processo de cifragem, e para restaurar informações cifradas para sua forma original, inteligível, através de um processo de decifragem. A criptografia também se preocupa com as técnicas de criptoanálise, que dizem respeito à formas de recuperar aquela informação sem se ter os parâmetros completos para a decifragem.
Criptografia Assimétrica	Tipo de criptografia que usa um par de chaves criptográficas distintas (privada e pública) e matematicamente relacionadas. A chave pública está disponível para todos que queiram cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente; a chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.
Criptografia de Chaves Públicas	Ver Criptografia Assimétrica
CSP (Cryptographic Service Provider)	Biblioteca de software que implementa a *Cryptographic Application Programming Interface (CAPI)*. CSP's implementam funções de codificação e decodificação, que os programas de aplicação de computador podem usar para, por exemplo, autenticação segura de usuário ou para o email seguro. CSP's são executados basicamente como um tipo especial de DLL com limitações especiais no carregamento e no uso.
Curvas Elípticas	Criptografia de curvas elípticas (ECC) é uma abordagem de criptografia de chave pública baseada na estrutura de curvas algébricas de campos finitos. As curvas elípticas são usadas também em diversos algoritmos de fatoração de inteiro que tem aplicações em criptografia.
Custódia	Responsabilidade jurídica de guarda e proteção de um ativo, independente de vínculo de propriedade. A custódia, entretanto, não permite automaticamente o acesso ao ativo, nem o direito de conceder

PALAVRA CHAVE	DESCRIÇÃO
	acesso a outros.
Dados	Informações representadas em forma digital, incluindo voz, texto, *fac-símile*, imagens e vídeo.
Dados de Ativação	Valores de dados, que não sejam chaves criptográficas, necessários para operar módulos criptográficos e que necessitam ser protegidos (ex.: PIN, *passphrase* ou uma chave compartilhada manualmente).
Data de validade do Certificado	A hora e a data de quando termina o período operacional de um certificado digital. Não tem relação com a revogação antes da hora e data anteriormente prevista.
Datação de Registros	Serviço de certificação da hora e do dia em que foi assinado um documento eletrônico, com identidade do autor.
Decifrar	Processo que transforma dados previamente cifrados e ininteligíveis de volta à sua forma legível.
Declaração das Práticas de Carimbo de Tempo (DPCT)	Declaração das práticas e dos procedimentos empregados pela ACT para emitir Carimbos do Tempo.
Declaração de Praticas de Certificação (DPC)	Documento, periodicamente revisado e republicado, que descreve as práticas e os procedimentos empregados pela Autoridade Certificadora na execução de seus serviços. É a declaração a respeito dos detalhes do sistema de credenciamento, as práticas, atividades e políticas que fundamentam a emissão de certificados e outros serviços relacionados. É utilizado pelas Autoridades Certificadoras para garantir a emissão correta dos certificados e pelos solicitantes e partes confiantes para avaliar a adequação dos padrões de segurança empregados às necessidades de segurança de suas aplicações.
Decriptografar	Ver Decifrar
DER (Distinguished Encoding Rules)	Regras para codificação de objetos ASN.1 em uma sequência de *bytes*. Corresponde a um caso especial de BER.
DES (Data Encryption Standard)	Algoritmo simétrico de criptografia de dados que utiliza um sistema de cifragem em blocos. Foi criado pela IBM em 1977 e apesar de permitir cerca de 72 quadrilhões de combinações (2^{56}), seu tamanho de chave (56 bits) é considerado pequeno, tendo sido quebrado por "força bruta" em 1997 em um desafio lançado na internet. Está definido no documento de padronização FIPS 46-1.

PALAVRA CHAVE	DESCRIÇÃO
Desastre	i. Evento súbito e inesperado cujo impacto resulta em perdas significativas para a organização. ii. Uma circunstância em que um negócio é julgado incapaz de funcionar em consequência de alguma ocorrência natural ou criada.
Desativação de Chave	Contrário de ativação de chave (ver Ativação de Chave).
Destruição de Chave	Eliminação física da mídia armazenadora e/ou lógica (sobrescrever os espaços onde a chave estiver armazenada) da chave criptográfica.
Diffie-Hellman	Método de criptografia desenvolvido por Whitfield Diffie e Martin Hellman e publicado em 1976. Permite que haja a troca de chaves públicas entre duas ou mais partes, permitindo que as pessoas que recebem a chave pública usem essa chave para cifrar o conteúdo de uma mensagem que será enviada à parte que forneceu a chave pública. Esse texto cifrado não poderá ser aberto por indivíduos que possuam a chave pública e sim, apenas pela parte que enviou a chave pública, pois a mesma possui a chave privada que se encontra em seu poder. Tendo posse dessa chave a mensagem cifrada poderá ser aberta.
Direito de Acesso	Privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.
Diretório	Unidade lógica de armazenamento que permite agrupar arquivos em pastas hierárquicas e subpastas.
Disponibilidade	Razão entre o tempo durante o qual o sistema está acessível e operacional e o tempo decorrido. No âmbito da ICP-Brasil a disponibilidade das informações publicadas pelas AC em serviço de diretório ou página *web* deve ser de 99% do mês, 24 horas por dia e 7 dias por semana.
DMZ (Demilitarized Zone)	Área na rede de uma empresa que é acessível à rede pública (internet), mas não faz parte da sua rede interna. Geralmente, esses servidores possuem números de IP acessíveis pela rede externa, o que os torna alvos de ataques. Para assegurar que os riscos são minimizados, um sistema de detecção e prevenção de intrusos deve ser implementado nessa DMZ.
DN (Distinguished Name)	Conjunto de dados que identifica de modo inequívoco uma entidade ou indivíduo pertencente ao mundo físico no mundo digital (por exemplo: país=BR, estado=Rio de Janeiro, nome organizacional=Sua Empresa S.A., nome comum=José da Silva).
DNS (Domain Name	Serviço e protocolo da família TCP/IP para o armazenamento e consulta

PALAVRA CHAVE	DESCRIÇÃO
Service)	às informações sobre recursos da rede. A implementação é distribuída entre diferentes servidores e trata principalmente da conversão de nomes internet em seus números IP correspondentes.
Documentação técnica	Conjunto de documentos técnicos que acompanham o objeto de homologação e que a parte interessada deve depositar no LSITEC-LEA para servir ao processo de homologação. A documentação técnica deve apresentar uma descrição técnica sobre o objeto de homologação que satisfaça aos requisitos definidos no MCT.
Documento	Unidade de registro de informações, qualquer que seja o suporte.
Documento digital	Unidade de registro de informações, codificada por meio de dígitos binários.
Documento Eletrônico	Unidade de registro de informações, acessível por meio de um equipamento eletrônico.
Drift	Variação no *skew* (segunda derivada do *offset*) apresentada por alguns relógios.
DSA (Digital Signature Algarithm)	Algoritmo unicamente destinado a assinaturas digitais, foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão DSS (*Digital Signature Standard)*. Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr. Foi inventado pela NSA e patenteado pelo governo americano.
ECB (Electronic Code Book)	Modo de operação de uma cifra de bloco (ver cifra de bloco), com a característica que cada bloco possível de "texto claro" tem um valor correspondente definido da mensagem cifrada e vice-versa. Ou seja o mesmo valor de "texto claro" resultará sempre no mesmo valor da mensagem cifrada. ECB é usado quando um volume de "texto claro" é dividido em diversos blocos dos dados, onde cada um é então cifrado independentemente de outros blocos. De fato, ECB tem a capacidade de suportar uma chave separada de cifração para cada tipo do bloco.
e-PING	Padrões de Interoperabilidade de Governo Eletrônico: define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de Serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela e-PING, estão segmentadas em: " Interconexão; " Segurança; " Meios de Acesso; " Organização e Intercâmbio de Informações; " Áreas e Assuntos de

PALAVRA CHAVE	DESCRIÇÃO
	Integração para Governo Eletrônico.
Elemento de Dado	No contexto da norma ISO/IEC 7816-4 referente ao cartão inteligente, um elemento de dado corresponde a um item de informação para o qual é associado um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4].
Emissão de Certificado Digital	Atividade de geração de um Certificado Digital, a inclusão neste dos dados de identificação do seu emissor (Autoridade Certificadora), do titular e da sua assinatura digital e subsequente notificação ao seu solicitante, observados os dispostos nos documentos públicos das AC denominados Práticas de Certificação - PC e Declaração de Práticas de Certificação – DPC.
Empresa de Auditoria Especializada e Independente	Vide Empresa de Auditoria Independente
Empresa de Auditoria Independente	Empresas, autorizadas pelo ITI para atuar na ICP-Brasil e que podem ser contratadas pelas autoridades certificadoras para realizar auditorias operacionais em entidades a elas subordinadas.
Encadeamento	Ato de associar um carimbo de tempo a outro.
Encriptar	Ver Cifrar
Engenharia Social	Termo utilizado para a obtenção de informações importantes de uma organização, através de seus usuários e colaboradores, ou de uma pessoa física. Essas informações podem ser obtidas pela ingenuidade ou confiança. Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e até mesmo pessoalmente.
Ensaio	Procedimento técnico realizado em conformidade com as normas aplicáveis, que objetiva analisar um ou mais requisitos técnicos de um dado sistema ou equipamento.
Entidade de Auditoria de Tempo (EAT)	Entidade que realiza as atividades de autenticação e sincronismo de Servidores de Carimbo do Tempo (SCT). Na estrutura de carimbo do tempo da ICP-Brasil, a EAT é a AC-Raiz, que possui Sistemas de Auditoria e Sincronismo (SASs) ligados diretamente ao relógio atômico.
Entidades Operacionalmente Vinculadas	Entidade relacionada a outra: i. como matriz, subsidiária, sócia, *joint-venture,* contratada ou agente, ii. como membro de uma comunidade de interesses registrada, ou

PALAVRA CHAVE	DESCRIÇÃO
	iii. como entidade que mantém relacionamento com uma entidade principal, que mantém negócios ou registros capazes de fornecer comprovação adequada da identidade da afiliada. No caso da ICP-Brasil, diz-se que uma AR ou PSS está operacionalmente vinculada a uma AC, por exemplo.
Entidade Usuária Externa	Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido.
Enveloped Data	Conteúdo cifrado de todos os tipos e chaves cifradas de sessão do tipo *"content-encryption"* para um ou mais recipientes. As mensagens *"enveloped"* mantêm os conteúdos do segredo da mensagem e reservam-nos somente a pessoas ou entidades para recuperar os conteúdos. *Cryptographic message syntax (CMS)* pode ser usado para codificar mensagens *"enveloped"*.
Equipamento de Certificação Digital	Aparelho, dispositivo ou elemento físico que compõe meio necessário ou suficiente à realização de Certificação Digital
Erro	Diferença de tempo medida entre os relógios de um SAS e de um SCT.
Erro Máximo Acumulado	Erro máximo que pode ser acumulado pelo relógio interno do SCT, entre duas ASR.
Esquema de Assinatura	Conjunto formado por um algoritmo de criação de assinatura, um algoritmo de verificação de assinatura e um algoritmo de geração de chaves, sendo que esse último gera chaves para os outros dois algoritmos.
Esquema de Envelopes Criptográficos	Combinação formada por uma cifra simétrica e uma cifra assimétrica. Os dados são cifrados com chave simétrica e esta é cifrada com a chave assimétrica pública
Estabilidade	Capacidade de um oscilador em manter a mesma frequência em um determinado intervalo de tempo.
***Escrow* de Chave Privada**	Vide Recuperação de Chave
Evento	Ocorrências de significância, eletrônicas ou manuais, que devem ser registradas para análises e auditorias posteriores. Na ICP-Brasil, há diversos tipos de eventos que devem obrigatoriamente ser registrados, como: iniciação e desligamento do sistema de certificação; tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC etc.
Exatidão	Afastamento máximo tolerado entre o valor indicado por um sistema de

PALAVRA CHAVE	DESCRIÇÃO
	medição e o valor verdadeiro do tempo.
Expoente Privado	Representa o expoente na definição de chave privada: par (d, n) onde "d" é o expoente privado e "n" é o módulo público (produto de dois fatores primos privados).
Expoente Público	Representa o expoente na definição de chave pública: par (e, n) onde "e" é o expoente público e "n" é o módulo público (produto de dois fatores primos privados).
Exportação de certificado digital	Atividade de copiar um Certificado Digital instalado em determinado computador ou hardware, para um disquete, CD, etc, permitindo a sua instalação em outro(s) computador(es) ou hardware.
Exportação de chaves criptográficas	Processo de retirada de chave criptográfica do módulo criptográfico. A exportação pode ser realizada de forma manual ou automática.
Exportação de chaves criptográficas de forma automática	Processo de retirada de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Exportação de chaves criptográficas de forma manual	Processo de retirada de chave criptográfica do módulo criptográfico que utiliza métodos manuais. Ex: apresentação do valor da chave um *display.*
***FIPS (Federal Information Processing Standards*)**	Correspondem aos padrões e diretrizes desenvolvidos e publicados pelo NIST (*National Institute of Standards and Technology*) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade e não há padrões ou soluções industriais aceitáveis.
FIPS 140 Federal Information Processing Standards)	O *Federal Information Processing Standards* 140 é um padrão do governo dos Estados Unidos para implementações de módulos de criptografia - ou seja, hardware e software para cifrar e decifrar dados ou realizar outras operações criptográficas (como geração ou verificação de assinaturas digitais). Encontra-se atualmente na versão 2, estando em elaboração, pelo NIST, a versão 3.
Firewall	Conjunto formado por Hardware, Software e uma política de acesso instalado entre redes, com o propósito de segurança. A função do *firewal*l é controlar o tráfego entre duas ou mais redes, com o objetivo de fornecer segurança, prevenir ou reduzir ataques ou invasões às bases de dados corporativas, a uma (ou algumas) das redes, que normalmente têm

PALAVRA CHAVE	DESCRIÇÃO
	informações e recursos que não devem estar disponíveis aos usuários da(s) outra(s) rede(s).
Firmware	Programas e componentes de dados de um módulo que estão armazenados em uma porção de hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) que não podem ser dinamicamente escritos ou modificados durante a execução.
Fonte Confiável de Tempo (FCT)	Denominação dada a um relógio sincronizado a hora UTC.
Fronteira criptográfica (*Cryptographic Boundary*)	Perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.
Função Resumo	Transformação matemática que mapeia uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resultado hash ou resumo criptográfico - de forma que seja muito difícil encontrar duas mensagens distintas produzindo o mesmo resultado hash (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado hash, não é possível recuperar a mensagem que o gerou).
Geração de Par de Chaves	Processo de criação de um par de chaves (chave privada e chave pública), sendo normalmente executado na solicitação de um certificado digital.
Gerador de Números Aleatórios	Vide *RNG*
Gerador de Números Pseudo-aleatórios	Vide *PRNG*
Gerenciamento de Certificado	Conjunto de procedimentos a partir do qual a AC, baseada em suas DPC, PC e PS, atua na emissão, renovação e revogação de certificados, bem como na emissão e publicação da sua LCR.
Gerenciamento de Risco	Processo que visa a proteção dos ativos das entidades integrantes da ICP-Brasil, por meio da eliminação, redução ou transferência dos riscos, conforme seja econômica e estrategicamente mais viável.
Hacker	Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.

PALAVRA CHAVE	DESCRIÇÃO
Handle	i. Dispositivo, unido a um objeto, que seja anexado para mover ou usar o objeto. ii. Tipo do ponteiro inteligente, uma referência a uma posição na memória de computador.
Hardware	i. Conjunto dos componentes físicos necessários à operação de um sistema computacional. ii. Equipamento mecânico e eletrônico, combinado com *software* (programas, instruções, etc.) na implementação de um sistema de processamento de informações eletrônicas.
Hardware Secure Module (HSM)	Dispositivo baseado em *hardware* que gera, guarda e protege chaves criptográficas, além de ter a capacidade de executar operações criptográficas, como assinatura digital.
Hash	Resultado da ação de algoritmos que fazem o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resultado *hash* - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um *hash*, não é possível recuperar a mensagem que o gerou).
Hibernação	Modo de operação *"power-saving"* que conserve a bateria do computador, mas permite uma reativação mais rápida da operação do que desligando o computador e então voltando a ligá-lo. Quando o modo de hibernação é ativado, todas as aplicações atuais que estão na memória estão conservadas no disco e o computador é desligado. Ao retomar a operação, pressionando uma tecla ou clicando o *mouse*, as aplicações são lidas do disco e voltam ao mesmo estado anterior.
Hierarquia do Certificado	Estrutura de certificados digitais que permite a indivíduos verificarem a validade de um certificado. O certificado é emitido e assinado por uma Autoridade Certificadora que está numa posição superior na hierarquia dos certificados. A validade de um certificado específico é determinada, entre outras coisas, pela validade correspondente ao certificado da AC que fez a assinatura.
Homologação	Processo que consiste no conjunto de atos, realizados de acordo com um Regulamento e com as demais normas editadas ou adotadas pela ICP-Brasil, que, se plenamente atendido, resultará na expedição de ato pelo qual, na forma e nas hipóteses previstas, a entidade responsável pela condução do referido processo reconhecerá o laudo de conformidade.

PALAVRA CHAVE	DESCRIÇÃO
HSM (Hardware Security Modules)	Vide Módulo de Segurança Criptográfica
IDEA (International Data Encryption Algorithm)	Algoritmo criado em 1991 por James Massey e Xuejia Lai e possui patente da suíça ASCOM Systec. O algoritmo é estruturado seguindo as mesmas linhas gerais do DES. Mas, na maioria dos microprocessadores, uma implementação por softw*are* do IDEA é mais rápida do que uma implementação por *software* do DES. O IDEA é o programa para criptografia de *e-mail* pessoal mais disseminado no mundo. Seu tamanho de chave é de 128 bits.
Identificação	Vide Autenticação
Identificador de Registro	Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4].
Importação de Certificado Digital	Atividade de copiar um Certificado Digital a partir de um disquete, CD, *smart card,* para um computador ou hardware, permitindo a sua instalação e uso posterior, por exemplo, para assinatura digital de *e-mails.*
Importação de chaves criptográficas	Processo de inserção de chave criptográfica no módulo criptográfico. A importação pode ser realizada de forma manual ou automática.
Importação de chaves criptográficas de forma automática	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza uma mídia eletrônica ou meio de comunicação eletrônico.
Importação de chaves criptográficas de forma manual	Processo de inserção de chave criptográfica de um módulo criptográfico que utiliza métodos manuais. Ex: digitação em um teclado, por uma entidade usuária externa, do valor da chave.
Incerteza	Dispersão dos valores que podem ser atribuídos a um mensurando, como resultado de uma sincronização.
Incidente de Segurança	Evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo das entidades integrantes da ICP-Brasil.
Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)	Conjunto de técnicas, arquitetura, organização, práticas e procedimentos, implementados pelas organizações governamentais e privadas brasileiras que suportam, em conjunto, a implementação e a operação de um sistema de certificação. Tem como objetivo estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em

PALAVRA CHAVE	DESCRIÇÃO
	criptografia de chave pública, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. A ICP-Brasil foi criada pela Medida Provisória 2200-2, de 24.08.2001 e está regulamentada pelas Resoluções do Comitê Gestor da ICP-Brasil, disponíveis no sítio www.iti.gov.br.
Instalação Técnica (IT)	Ambiente físico de uma AR, cujo funcionamento foi autorizado pelo ITI, por tempo indeterminado, onde serão realizadas as atividades de validação e verificação da solicitação de certificados.
Instalação Técnica Secundária (ITS)	Ambiente físico de uma AR vinculada à Instalação Técnica, cujo funcionamento foi devidamente autorizado pelo ITI, onde é realizada exclusivamente a atividade de coleta e/ou verificação biométrica e validação da solicitação de certificados
Instituto Nacional de Tecnologia da Informação (ITI)	Autarquia federal vinculada à Casa Civil da Presidência da República, é a Autoridade Certificadora Raiz da ICP-Brasil. É a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.
Integridade	Garantia oferecida ao usuário de que documento eletrônico, mensagem ou conjunto de dados não foi alterada, nem intencionalmente, nem acidentalmente por pessoas não autorizadas durante sua transferência entre sistemas ou computadores.
Interface	Ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos softwares.
Intimação	Ato pelo qual se dá conhecimento do procedimento de fiscalização para que a entidade fiscalizada faça ou deixe de fazer alguma coisa.
Irretratabilidade	Mecanismo para garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.
IRIG (Inter-range instrumentation group time codes)	Formatos para codificação do tempo definidos pelo Telecommunications and Timing Group (TTG) of the Range Commanders Council (RCC).
ISO (International Standards Organization)	Organização que cria padrões internacionais para diversas áreas, incluindo computadores. Congrega em torno de 90 países.

PALAVRA CHAVE	DESCRIÇÃO
ITU (International Telecommunication Union)	Organização internacional que faz parte do Sistema das Nações Unidas. Responsável pelo estabelecimento de normas e padrões em telecomunicações e seus serviços.
Key Containers	Parte do *key database* (banco de dados que contém as chaves criptográficas para um *CSP* específico) que contém todos os pares de chaves (pares de chaves para troca e assinatura) que pertencem a um usuário específico. Cada recipiente tem um nome único que é usado ao chamar funções de contexto para obter um *handle* ao *container*.
Key Zeroization	Método de apagar chaves criptográficas armazenadas eletronicamente, alterando ou suprimindo os índices de armazenamento das chaves para impedir a recuperação das informações.
Laboratório de Ensaio e Auditoria (LEA)	Entidades, formalmente vinculadas ao ITI, aptas a realizar os ensaios exigidos nas avaliações de conformidade e a emitir os correspondentes laudos de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil, que embasarão a tomada de decisão por parte do ITI quanto à homologação ou não de um dado sistema ou equipamento avaliado.
Laudo de Conformidade	Documento emitido ao final da avaliação de conformidade, na forma prevista na resolução nº 36 do CG da ICP-Brasil , que atestará se um dado sistema ou equipamento, devidamente identificado, está ou não em conformidade com as normas editadas ou adotadas pela ICP-Brasil.
Leap second	Segundo adicionado ao UTC para compensar o atraso da rotação da Terra e manter o UTC em sincronismo com o tempo solar.
Leitora de Cartão Inteligente	Hardware instalado no computador, utilizando de interface serial ou usb, que serve para efetuar leituras de *smart cards.*
Lista de Certificados Revogados (LCR)	Lista assinada digitalmente por uma Autoridade Certificadora, publicada periodicamente, contendo certificados que foram revogados antes de suas respectivas datas de expiração. A lista, geralmente, indica o nome de quem a emite, a data de emissão e a data da próxima emissão programada, além dos números de série dos certificados revogados e a data da revogação.
Lista de Controle de Acesso	Lista de indivíduos ou entidades com permissão de acesso a certas áreas específicas de um servidor, rede, aplicação de internet ou instalações físicas.
Log	Conjunto de registros que lista as atividades realizadas por uma máquina ou usuário específico. Um único registro é conhecido como 'registro de log'. Em termos de segurança, os *logs* são usados para identificar e

PALAVRA CHAVE	DESCRIÇÃO
	investigar as atividades suspeitas e estudar as tentativas (ou os sucessos) dos ataques, para conhecimento dos mecanismos usados e aprimoramento do nível de eficiência da segurança.
Login	Processo de identificação e autenticação ao qual o usuário é submetido antes de integrar ao sistema, software ou aplicativo.
Logoff	Processo de encerramento da sessão de trabalho pelo usuário.
MAC (Message Authentication Code)	Pequena parte de informação usada para autenticar uma mensagem. Um algoritmo MAC aceita como entrada uma chave secreta e uma mensagem de comprimento indefinido para ser autenticado e envia como saída um MAC (conhecido às vezes como *tag)*. O valor do MAC protege a integridade de uma mensagem assim como sua autenticidade, permitindo que os verificadores (quem possuem também a chave secreta) detectem todas as mudanças no conteúdo da mensagem.
Método de *Padding*	Processo de inserção de bits numa mensagem, preparando-a para a cifração ou assinatura.
MD5 *(Message Digest 5)*	Função de *hash,* ou resumo de mensagem - espalhamento unidirecional - inventada por Ron Rivest. Este algoritmo produz um valor *hash* de 128 bits, para uma mensagem de entrada de tamanho arbitrário. Foi inicialmente proposto em 1991, após alguns ataques de criptoanálise terem sido descobertos contra a função *hashing* prévia: a MD4. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza em parte do MD5, mas até agora ela não afetou a segurança global do algoritmo. Entretanto, o fato dele produzir um valor *hash* de somente 128 bits é o que causa maior preocupação.
Mídia	Base física (*hardware*) ou lógica (*software*) sobre a qual a informação é registrada, podendo ser exportada para outra mídia ou permanecer armazenada nela própria.
Mídia Armazenadora	Vide Mídia.
MIME (Multipurpose Internet Mail Extensions)	Padrão da internet que estende o formato de *e-mail* para suportar: texto em conjunto de caracteres além do tipo *US-ASCII*; anexos do tipo *não-texto*; corpos de mensagem do tipo *multi-part* e informação de cabeçalho em conjunto de caracteres do tipo *não-ASCII.* Os tipos de conteúdo definidos por padrões MIME são também de importância além do *e-mail*, como em protocolos de comunicação como

PALAVRA CHAVE	DESCRIÇÃO
	o HTTP para a internet.
Mitigação	Conjunto de ações para minimizar ameaças, evitando que estas venham a se tornar desastres. Estas ações também reduzem os efeitos dos desastres. A mitigação focaliza em medidas a longo prazo para se reduzir ou eliminar os riscos no ambiente considerado.
Modo de Operação	Tipo de tratamento que será dado aos blocos de mensagem, para evitar que blocos idênticos gerem o mesmo resultado criptográfico ao serem cifrados.
Módulo Criptográfico	Software ou hardware que fornece serviços criptográficos, como cifração, decifração, geração de chaves, geração de números aleatórios.
Módulo criptográfico mono-CI	Módulo criptográfico com um único circuito integrado protegido por um invólucro.
Módulo criptográfico multi-CI	Módulo criptográfico com vários circuitos integrados protegidos por um invólucro.
Módulo criptográfico multiaplicação	Módulo criptográfico que suporta mais que uma aplicação. Exemplo: módulo criptográfico contendo aplicação ICP e aplicação EMV.
Módulo de Segurança Criptográfica (MSC)	*Hardware* com capacidade de processamento, que gera chaves criptográficas e assina documentos, sendo usado para para assinar os certificados digitais em Autoridades Certificadoras, oferecendo grande velocidade e segurança.
Multi-threaded	Característica dos sistemas operativos modernos que permite repartir a utilização do processador entre várias tarefas simultaneamente.
Não-repúdio	Garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital. Deste modo, a menos de um uso indevido do certificado digital, fato que não exime de responsabilidade, o autor não pode negar a autoria da transação. Transações digitais estão sujeitas a fraude, quando sistemas de computador são acessados indevidamente ou infectados por cavalos-de-tróia ou vírus. Assim os participantes podem, potencialmente, alegar fraude para repudiar uma transação.
Navegador de internet ou *Browser*	Aplicativo utilizado para visualizar arquivos HTML, VRML, textos, arquivos de áudio, animação, videoclipes e/ou correio eletrônico pela internet. Entre os principais navegadores disponíveis no mercado estão:

PALAVRA CHAVE	DESCRIÇÃO
	Microsoft Internet Explorer, Netscape Navigator, Opera, Mozilla, etc.
NBR (Norma Brasileira Regulamentadora)	É a sigla de Norma Brasileira aprovada pela ABNT, de caráter voluntário e fundamentada no consenso de um grupo de representantes da comunidade científica. Suas disposições abrangem diversos temas e são obrigatórias quando em condições estabelecidas pelo poder público competente.
Negociação de chaves (*Key Agreement*)	Processo ou protocolo que possibilita atribuir uma chave criptográfica simétrica compartilhada aos parceiros legítimos em função de valores secretos escolhidos por cada um dos parceiros, de forma que nenhuma outra entidade possa determinar o valor da chave criptográfica. Exemplo clássico de negociação de chaves é o algoritmo *Diffie-Hellman*.
No-breaks	Equipamento que tem como função suprir a energia de um circuito, por um tempo determinado, na ausência da fonte de energia principal da rede elétrica.
Nome Significativo	Nome que determinar a identidade da pessoa ou organização a que se refere.
Número de Série do Certificado	Valor que identifica de forma unívoca um certificado emitido por uma Autoridade Certificadora.
Número de Identificação Pessoal (*Personal Identification Number* - PIN)	Código alfanumérico ou senha usada para autenticar uma identidade.
Número de Registro	No contexto do sistema de arquivos de cartões inteligentes, é um número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4].
***Object Identifier* (OID)**	Número único que identifica uma classe de objetos ou um atributo em um diretório ou combinação de diretórios. OIDs são definidos por entidades emissoras e formam uma hierarquia. Um OID é representado por um conjunto de números decimais separados por pontos (ex.: 1.2.3.4). OIDs são usados extensivamente em certificados de formato X.509, como por exemplo, para designar algoritmos criptográficos empregados, políticas de certificação e campos de extensão. Praticamente toda implementação de ICP usando este formato requer o registro de novos OIDs, em particular uma que designe a política de certificação que

PALAVRA CHAVE	DESCRIÇÃO
	estabelece seu regime regulatório básico. É crucial que os OIDs sejam obtidos dos legítimos responsáveis pelos arcos, para se evitar incompatibilidades e colisões. Nos certificados da ICP-Brasil os OIDs utilizados para identificar as Políticas de Certificados e Declaração de Práticas de Certificação das Autoridades Certificadoras são atribuídos pelo ITI, durante o processo de auditoria da AC e obedecem a seguinte lógica: **2.16.76.1.1.n –** OID para Declarações de Práticas de Certificação **2.16.76.1.2.n –** OID para Políticas de Certificados **2.16.76.1.3.n e 2.16.76.1.4.n –** OID usados para permitir a inclusão no certificado de outros dados de pessoas físicas e jurídicas, como CNPJ, CPF, título de eleitor, categoria profissional etc.
Objeto de Dado	No contexto do padrão ISO/IEC 7816-4 para cartões inteligentes, um objeto de dado consiste em um conjunto de caracteres (*tag*), um comprimento e um valor (um elemento de dado, por exemplo). Nesta parte do padrão ISO/IEC 7816, objetos de dados são referenciados como BER-TLV, COMPACT-TLV e SIMPLE-TLV [ISO/IEC 7816-4].
Observatório Nacional (ON)	Unidade de pesquisa do Ministério da Ciência e Tecnologia (MCT), integrante do Sistema Nacional de Metrologia (SINMETRO). O ON é o responsável legal pela geração, conservação e disseminação da Hora Legal do Brasil.
Octeto	Conjunto de 8 bits compreendendo um *byte*.
OCSP (On-line Certificate Status Protocol)	Protocolo para verificação de Estado de Certificado *On-line,* OCSP é um dos dois esquemas comuns para verificar se um certificado digital não se encontra revogado. O outro método é a LCR (ver LCR). Através do OCSP, qualquer aplicação pode fazer consultas a um serviço que checa, diretamente no Banco de Dados da Autoridade Certificadora, o status de um determinado certificado. As respostas emitidas por este serviço são individuais (uma para cada certificado) e são assinadas digitalmente, a fim de garantir sua confiabilidade. Dessa maneira, a lacuna entre o momento da revogação e a emissão da próxima LCR deixa de existir, já que, uma vez que seja marcado como revogado no banco de dados da AC, a próxima resposta OCSP já apresentará este status, eliminando a possibilidade de um acesso não-autorizado desta natureza.
Off-Line	Fora de linha, desligado. Quando não existe nenhum contato do computador com uma rede.

PALAVRA CHAVE	DESCRIÇÃO
Oficial de Segurança	Perfil de acesso que permite a uma entidade usuária externa realizar serviços relacionados à iniciação do sistema de arquivos do módulo, gerenciamento do módulo, reinicialização do módulo, sobrescrita do valor de chaves criptográficas (*key zeroization*) e destruição do módulo.
On-Line	Significa "estar em linha", estar ligado em determinado momento à rede ou a um outro computador.
Operação Criptográfica	Operação que manipula uma chave criptográfica.
Operador	Indivíduo ou processo que realiza operações no módulo criptográfico.
OpenSSL	Implementação de código aberto dos protocolos SSL e TLS. A biblioteca (escrita na linguagem C) implementa as funções básicas de criptografia e disponibiliza várias funções utilitárias. O *OpenSSL* está disponível para a maioria dos sistemas do tipo Unix, incluindo Linux, Mac OS X e para as quatro versões do BSD de código aberto e também para o *Microsoft Windows.*
Par de chaves	Chaves privada e pública de um sistema criptográfico assimétrico. A chave privada e sua chave pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da chave privada a partir da chave pública conhecida. A chave pública pode ser usada para verificação de uma assinatura digital que a chave privada correspondente tenha criado ou a chave privada pode decifrar a uma mensagem cifrada a partir da sua correspondente chave pública. A chave privada deve ser de conhecimento exclusivo do titular do certificado.
Parâmetros críticos de segurança (PCS)	Representam informações sensíveis e relacionadas à segurança, tais como, chaves criptográficas assimétricas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja leitura ou modificação podem comprometer a segurança de um módulo criptográfico.
PEM (Privacy Enhanced Mail)	Padrão da Internet que fornece troca segura no correio eletrônico. O PEM emprega um conjunto de técnicas de criptografia para permitir a confidencialidade, a autenticação do remetente e a integridade da mensagem. Os aspectos da integridade da mensagem permitem que o usuário assegure de que uma mensagem não seja modificada durante o transporte do remetente.

PALAVRA CHAVE	DESCRIÇÃO
	A autenticação do remetente permite que um usuário verifique que a mensagem PEM que receberam é verdadeiramente da pessoa que reivindica tê-la emitido. A característica da confidencialidade permite que uma mensagem seja mantida secreta das pessoas a quem a mensagem não foi dirigida.
PI (Parte Interessada)	Parte interessada (empresa) que deseja fazer a homologação junto ao LSITEC-LEA.
PIN (Personal Identification Number)	Sequência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas.
PKCS (Public Key Cryptographic Standard)	Padrões de criptografia de chave pública. São especificações produzidas pelos Laboratórios RSA em cooperação com desenvolvedores de sistemas seguros de todo o mundo com a finalidade de acelerar a distribuição da criptografia de chave pública.
PKCS#1	Especificação de padrão de dados para o protocolo RSA, incluindo o padrão para criptografia e assinatura digital RSA e o padrão para estocagem de chaves públicas e privadas.
PKCS#5	Especificação de um padrão para derivação de chaves e mecanismos de cifração baseado em senhas. Descreve um método para cifrar um vetor de bytes utilizando uma chave secreta calculada a partir de uma senha (*Password-Based Encryption* ou PBE). É destinado á proteção de chaves privadas em situações que exijam a sua transferência. Isto pode ser necessário, por exemplo, quando as chaves são geradas pela CA e não pelo usuário; ou quando o usuário necessita transferir a chave para outra máquina. A cifragem utilizada está baseada no DES.
PKCS#10	Especificação de um padrão para codificar requisições de certificados, incluindo o nome da pessoa que requisita o certificado e sua chave pública.
PKCS#7 (CMS)	Padrão que descreve uma sintaxe genérica para dados que podem ser submetidos a funções criptográficas, tais como assinatura e envelopagem digital. Permite recursividade, com aninhamento de envelopes e *wrappers*. Permite também a associação de atributos arbitrários, como, por exemplo, selo temporal ou contra-assinatura, à mensagem no processo de autenticação por assinatura. Casos particulares oferecem meios de disseminação de certificados e CRLs. O CMS fornece suporte a uma variedade de arquiteturas de gerenciamento de chaves baseadas em ICP, como aquela proposta para o

PALAVRA CHAVE	DESCRIÇÃO
	padrão PEM na RFC 1422. Entretanto, topologias, modelos de confiança e políticas de certificação para ICPs estão fora do seu escopo. Valores produzidos pelo padrão estão destinados à codificação DER, ou seja, para transmissão e armazenagem na forma de cadeias de octetos de comprimento não necessariamente conhecidos de antemão. Na ICP-Brasil, é largamente utilizado na assinatura digital.
PKCS#8	Especificação de um padrão para chaves privadas: o valor da chave, o algoritmo correspondente e um conjunto de atributos associados. Define também em uma sintaxe para chaves cifradas recorrendo às técnicas PBE definidas no PKCS#5.
PKCS#11	Descreve a interface de programação chamada *"Cryptoki"* utilizada para operações criptográficas em hardwares: *tokens, smart cards*. É comum utilizar o PKCS#11 para prover o suporte aos *tokens* como as aplicações de SSL e S/MIME.
PKCS#12	Descreve uma sintaxe para a transferência de informação de identificação pessoal, incluindo chaves privadas, certificados, chaves secretas e extensões. É uma norma muito útil uma vez que é utilizada por diversas aplicações (ex. IE e Mozilla) para importar e exportar este tipo de informação. Suporta a transferência de informação pessoal em diferentes condições de manutenção da privacidade e integridade. O grau de segurança mais elevado prevê a utilização de assinaturas digitais e cifras assimétricas para proteção da informação.
PKI (Public Key Infrastrusture)	Infraestrutura de chaves públicas. A ICP-Brasil é um exemplo de PKI.
Plano de Auditoria	Roteiro que descreve, pelo menos, como a auditoria pretende proceder à verificação da Política de Certificação, PC, da Declaração de Práticas de Certificação, DPC e da Política de Segurança, PS e recomendar providências quanto às observações levantadas.
Plano de Contingência	Plano de ações para situações de emergência. Tem como objetivo a garantia da disponibilidade dos recursos e serviços críticos e facilitar a continuidade de operações de uma organização. Deve ser regularmente atualizado e testado, para ter eficácia caso necessária sua utilização. Sinônimo de plano de desastre e plano de emergência.
Plano de Continuidade de Negócios	Plano cujo objetivo é manter em funcionamento os serviços e processos críticos das entidades integrantes da ICP-Brasil, na eventualidade da

PALAVRA CHAVE	DESCRIÇÃO
	ocorrência de desastres, atentados, falhas e intempéries.
Plano de Desenvolvimento e Implantação dos Trabalhos de Auditoria	Plano elaborado pela Empresa de Auditoria Independente, que especifica de maneira clara e objetiva cada etapa do trabalho, procedimentos e técnicas a serem adotadas em cada atividade, prazo de execução e pontos de homologação, bem como tabelas indicativas do número de horas de auditoria e o número de auditores a serem alocados nos serviços que serão realizados em entidades da ICP-Brasil.
Plano de Recuperação de Desastres	Conjunto de procedimentos alternativos, a serem adotados após um desastre, visando a reativação dos processos operacionais que tenham sido paralisados, total ou parcialmente, ainda que com alguma degradação.
Política de Carimbo de Tempo (PCT)	Conjunto de normas que indicam a aplicabilidade de um carimbo de tempo para uma determinada comunidade e/ou classe de aplicação com requisitos comuns de segurança.
Política de Certificação (PC)	Documento que descreve os requisitos, procedimentos e nível de segurança adotados para a emissão, revogação e gerenciamento do ciclo de vida de um Certificado Digital.
Política de Segurança (PS)	Conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.
Posto Provisório	Ambiente montado pela AR, fora de suas instalações técnicas, para realização das atividades inerentes às autoridades de registro. Possui período de tempo determinado para funcionamento.
Precisão	Ver Exatidão.
Prestador de Serviço Biométrico (PSBio)	Entidade com capacidade técnica para realizar a identificação biométrica de acordo com os padrões internacionais.
Prestador de Serviço de Confiança (PSC)	Qualquer entidade credenciada junto à ICP-Brasil que forneça serviços de certificação.
Prestador de Serviço de Confiança de Armazenamento de Chaves Criptográficas	É uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de armazenamento de chaves privadas para usuários finais.
Prestador de Serviço de Confiança de Assinatura Digital	É uma entidade credenciada, auditada e fiscalizada pelo ITI que provê serviços de assinaturas e verificações de assinaturas digitais padrão ICP-Brasil nos documentos e transações eletrônicas ou ambos

PALAVRA CHAVE	DESCRIÇÃO
Prestador de Serviços de Suporte (PSS)	Entidade que desempenha as atividades descritas na PC, PCT, DPC ou DPCT da AC ou ACT, responsável por esses documentos. São empresas contratadas por uma AC, ACT ou AR para realizar atividades de: disponibilização de Infraestrutura física, lógica, e humana; ou quaisquer destes.
Privacidade de documentos eletrônicos	Vide Confidencialidade de Documentos Eletrônicos
PRNG (Pseudo Random Number Generator)	Algoritmo usado na geração de seqüências numéricas, cujos números são aproximadamente independentes um dos outros. A saída da maioria dos geradores de números aleatórios não é verdadeiramente aleatória; ela somente aproxima algumas das propriedades dos números aleatórios. Enquanto números verdadeiramente aleatórios podem ser gerados usando hardware para geração de número aleatório, número pseudo aleatórios são uma parte crítica da computação moderna, da criptografia até o método de *Monte Carlo* passando por sistemas de simulação. Uma cuidadosa análise matemática é necessária para assegurar que a geração dos números seja suficientemente "aleatória".
Procedimento de Fiscalização	Ações que objetivam a verificação do cumprimento das normas que regem a ICP-Brasil por parte das entidades credenciadas.
Protocolo	Descrição das regras que dois computadores devem obedecer ao estabelecer uma comunicação. Um conjunto de regras padronizadas que especifica o formato, a sincronização, o seqüenciamento, a transmissão de dados, incluindo inicialização, verificação, coleta de dados, endereçamento e verificação e correção de erros em comunicação de dados.
PSC (Provedor de Serviços Criptográficos)	Vide *CSP (Cryptographic Service Provider)*
Proxy	Servidor que age como um intermediário entre uma estação de trabalho e a internet para segurança, controle administrativo e serviço de *cache*. Um servidor (programa) *proxy* (ou com capacidades de *proxy*) recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua esses mesmos pedidos ao exterior dessa rede, usando como identificação o seu próprio numero IP e não o numero IP do computador que requisitou o serviço. Útil quando não se dispõe de números IP registrados

PALAVRA CHAVE	DESCRIÇÃO
	numa rede interna ou por questões de segurança.
PUK (Personal Identification Number Umblocking Key)	Chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens* e *smart cards*, o acesso à chave privada de um titular de certificado.
Rastreabilidade	Relacionamento do resultado de uma medição de sincronismo com um valor de referência previamente estabelecido como padrão. A rastreabilidade se evidencia por intermédio de uma seqüência contínua de medidas, devidamente registradas e armazenadas e permite a verificação, direta ou indireta, do relacionamento entre o tempo informado e a fonte confiável de tempo.
Recuperação de Chave	Processo no qual uma chave privada pode ser recuperada, a partir de dados armazenados por uma empresa ou órgão governamental. Na ICP-Brasil é proibida a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.
Rede	Grupo de computadores inter-conectados, controlados individualmente, junto com o hardware e o software usado para conectá-los. Uma rede permite que usuários compartilhem dados e dispositivos periféricos como impressoras e mídia de armazenamento, troquem informações por meio do correio eletrônico e assim por diante.
Rede de Carimbo do Tempo da ICP-Brasil	Rede criada e mantida pela AC-Raiz da ICP-Brasil, que se liga ao Observatório Nacional para obter a hora UTC e a dissemina às ACTs credenciadas na ICP-Brasil.
Rede de Sincronismo Autenticado (ReTemp/ HLB)	Rede criada e mantida pelo Observatório Nacional, que permite a rastreabilidade e a autenticação do tempo, nos equipamentos que a compõem, em relação à Hora Legal Brasileira e à UTC.
Rede Local	Grupo de computadores conectados com a finalidade de compartilhar recursos. Os computadores em uma rede local são normalmente ligados por um único cabo de transmissão e localizados dentro de uma pequena área, como um único prédio ou seção de um prédio.
Redundância	i. Componentes de um sistema de computador que são instalados para fazer *backup*. Utilizados para garantir a operação ininterrupta de um sistema em caso de falha. ii. Segundo dispositivo que esteja imediatamente disponível para uso

PALAVRA CHAVE	DESCRIÇÃO
	quando de uma falha de um dispositivo primário de um sistema de computador.
Registro	Cadeia de octetos que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].
Relatório de auditoria	Documento que traduz a forma como foi desenvolvido o trabalho de auditoria e que exprime de forma clara, concisa e exata, uma opinião sobre os resultados a que o auditor chegou, devendo conter, sempre que for caso, as alegações, as respostas ou as observações dos responsáveis e, ainda, conclusões e recomendações.
Relatório de Fiscalização	Documento pelo qual o servidor responsável pela fiscalização descreve o que constatou na entidade fiscalizada
Relying Party	Vide Terceira Parte
RNG (Random Number Generator)	Quando um número aleatório é gerado por um programa, este número não é exatamente aleatório (por isto que números aleatórios gerados por programas são mais corretamente classificados como pseudo-aleatórios). Portanto, em sistemas onde são geradas chaves criptográficas importantes, é necessário existir um circuito chamado *Random Number Generator* (RNG) que garanta que os números gerados são realmente ao acaso e não baseados no relógio de tempo real do computador.
Realimentação de dados de autenticação *(Echo)*	Exibição visível de caracteres no momento da inserção de uma senha.
Renovação de Certificados	Processo para obter um certificado novo antes que o certificado existente tenha expirado. Na ICP-Brasil, é obrigatória a geração de novas chaves criptográficas para cada certificado emitido.
Repositório	Sistema confiável e acessível *on-line,* mantido por uma Autoridade Certificadora, para publicar sua Declaração de Práticas de Certificação (DPC), Políticas de Certificado (PC), Política de Segurança (PS), Lista de Certificados Revogados (LCR) e endereços das instalações técnicas das AR vinculadas.
Resolução (*Resolution*)	Menor diferença entre indicações de um dispositivo mostrador que pode ser significativamente percebida. A resolução de um relógio é o menor incremento de tempo que o mesmo pode indicar.
Retardo (*Delay*)	Tempo de propagação na internet entre o SCT e o SAS.

PALAVRA CHAVE	DESCRIÇÃO
Revogação de Certificados	Encerramento da validade de um certificado digital antes do prazo previsto. Pode ocorrer por iniciativa do usuário, da Autoridade de Registro, da Autoridade Certificadora ou da Autoridade Certificadora Raiz.
RFC (Request for Comments)	Documentos técnicos ou informativos que discutem os mais diversos aspectos relacionados à internet. Os assuntos variam desde especificações, padrões e normas técnicas até questões históricas acerca da rede mundial de computadores. Os RFC são documentos públicos, qualquer pessoa tem acesso a eles, podendo ler, comentar, enviar sugestões e relatar experiências sobre o assunto. Pode-se pesquisar os RFC no *site*: http://www.faqs.org/rfcs.
Risco ou Ameaça	i. Probabilidade da concretização de um evento que possa causar perdas significativas por causar danos a um ou mais aos ativos da organização. ii. Fator externo que pode vir a atacar um ativo causando um desastre ou perda significativa.
Roteador	Sistema computacional que usa uma ou mais métricas para determinar o caminho otimizado pelo qual o tráfego da rede deve ser encaminhado – por meio de seus endereços – de uma rede local ou remota para outra.
Roteamento	Processo de seleção de rotas para uma mensagem.
RSA (Rivest Shamir and Adleman)	Algoritmo assimétrico que possui esse nome devido a seus inventores: Ron Rivest, Adi Shamir e Len Adleman, que o criaram em 1977 no MIT. É, atualmente, o algoritmo de chave pública mais amplamente utilizado, sendo capaz de fornecer assinaturas digitais e cifrar textos.
Sala-cofre	Área de Segurança restrita, formada por cofre com proteção eletromagnética, física e contra fogo, afim de proteger as chaves privativas que assinam os Certificados Digitais.
***Secure Messaging* (Transferência Segura de Mensagens por Meios Eletrônicos)**	Qualquer método de entrega de uma mensagem segura, incluindo *TLS* (segurança da camada de transporte), SMTP sobre SSL e HTTPS.
Segundo de Transição *(leap second)*	Ajuste ao UTC por meio da subtração ou adição de um segundo no último segundo de um mês do UTC. A primeira escolha é o fim de dezembro e de junho e a segunda escolha é o fim de março e de setembro.
Segurança Física	O principal objetivo da implantação de controles de segurança física é

PALAVRA CHAVE	DESCRIÇÃO
	restringir o acesso às áreas críticas da organização, prevenindo os acessos não autorizados que podem acarretar danos a equipamentos, acessos indevidos à informação, roubos de equipamentos, entre outros. Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico. A falta de implementação desses dois controles em conjunto, seria o mesmo que restringir o acesso às informações através de senhas, mas deixar os servidores desprotegidos fisicamente, vulneráveis a roubo, por exemplo.
Selo Cronológico Digital	Serviço que registra, no mínimo, a data e a hora correta de um ato, além da identidade da pessoa ou equipamento que enviou ou recebeu o selo cronológico. O Selo Cronológico Digital cria uma confirmação assinada digitalmente e à prova de fraude sobre a existência de uma transação ou documento específico.
Selo de Homologação	Selo conferido aos sistemas e equipamentos homologados pelo ITI.
Semente (de chave criptográfica)	Valor secreto usado para inicializar uma função ou uma operação criptográfica.
Senha	Conjunto de caracteres, conhecidos apenas pelo usuário, que fornecem acesso ao arquivo, computador ou programa. Senhas são geralmente usadas em conjunto com o nome do usuário que o autentica e o garante autorização ao acesso.
Senha Forte	Inverso de Senha Fraca ou Óbvia
Senha Fraca ou Óbvia	É aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tal como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras
Serviço Criptográfico ICP (ou Aplicação ICP)	Aplicação de Infraestrutura de chaves públicas contextualizada para o âmbito da ICP-Brasil.
Servidor de Aplicativos	Sistema que realiza a interface entre o subscritor e o SCT. Encaminha as solicitações de carimbo de tempo ao SCT e em seguida devolve ao subscritor os carimbos de tempo ou mensagens de erro recebidos em resposta.
Servidor de Auditoria e Sincronismo (SAS)	Dispositivo constituído por *hardware* e *software* que audita e sincroniza SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.

PALAVRA CHAVE	DESCRIÇÃO
Servidor de Carimbo do Tempo (SCT)	Dispositivo único constituído por *hardware* e *software* que gera os carimbos do tempo, sob o gerenciamento da ACT. Deve possuir um HSM contendo um relógio a partir do qual são emitidos os carimbos do tempo. Nesse HSM devem ser também realizadas as funções criptográficas de geração de chaves e assinaturas digitais.
SHA-1 (*Secure Hash Algorithm)*	O *Secure Hash Algorithm,* uma função de espalhamento unidirecional inventada pela NSA, gera um valor *hash* de 160 bits, a partir de um tamanho arbitrário de mensagem.
SHA-224, SHA-256,SHA-384 e SHA-512 (SHA-2 Family - Secure Hash Algorithm)	O NIST publicou quatro funções adicionais da família *SHA*, cada uma com valores *hash* maiores, conhecidos coletivamente como *SHA-2*. As variantes individuais são nomeadas, através de seus comprimentos de *hash* (em *bits*): SHA-224, SHA-256, SHA-384, e SHA-512. O SHA-224 foi definido para combinar o comprimento da chave com duas chaves TripleDES. SHA-256 e SHA-512 são funções de *hash* computadas com palavras de 32 bits e 64 bits respectivamente. Usam quantidades diferentes de deslocamento e constantes adicionais, mas suas estruturas são virtualmente idênticas, diferindo somente no número de voltas. SHA-224 e SHA-384 são simplesmente versões truncadas das duas primeiras, computadas com valores iniciais diferentes.
Sigilo	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas. Os titulares de certificados de assinatura digital emitidos pela AC são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves.
Signatário	Pessoa/entidade que cria uma assinatura digital para uma mensagem com a intenção de autenticá-la.
Signed Data	Qualquer conteúdo assinado. Um determinado número de assinantes pode assinar em paralelo qualquer tipo de conteúdo. A aplicação típica do tipo de conteúdo *signed data* é representada por uma assinatura digital do assinador no conteúdo do tipo de conteúdo de dados. Uma outra aplicação típica disseminada são os certificados digitais e as listas da revogação do certificado (CRL).
Sincronização de Relógio	Processo pelo qual dois ou mais relógios passam a indicar o mesmo tempo.
Sistema de	Dispositivo constituído por hardware e software que audita e sincroniza

PALAVRA CHAVE	DESCRIÇÃO
Autenticação e Sincronismo (SAS)	SAS ou SCT. Deve possuir um HSM com relógio para sincronização e capacidade de processamento criptográfico para geração de chaves criptográficas e realização de assinaturas digitais.
Sistema Autônomo (*Autonomous System* - AS)	Grupo de redes de endereço IP que é gerenciado por um ou mais operadores de rede de Internet, que possuem uma clara e única política de roteamento.
Sistema Criptográfico	Sistema composto de documentação normativa específica de criptografia aplicada na ICP-Brasil, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas.
Sistema de Certificação Digital	Programa de computador, ainda que embarcado, que possua meio necessário ou suficiente à realização de Certificação Digital.
Sistema de Detecção de Intruso (IDS)	Ferramentas de segurança que ajudam os administradores a evitarem danos na rede quando as outras proteções, tais como controle de acesso ou *firewalls*, não conseguem afastar os intrusos. Detecta tentativas ou ataques bem-sucedidos nos recursos monitorados. Os recursos monitorados podem fazer parte de uma rede ou um sistema *host*.
Sistema de Pagamento Brasileiro (SPB)	Sistema responsável pela interação entre o Banco Central, o governo, as instituições financeiras, as empresas e até mesmo as pessoas físicas. Gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, ligando as Instituições Financeiras credenciadas ao Banco Central do Brasil. Utiliza certificados digitais da ICP-Brasil para autenticar e verificar a identidade dos participantes em todas as operações realizadas;
Sistema Operacional	Programa principal que se dedica às tarefas de organização e controle das atividades do computador e seus periféricos.
Skew	Diferença de freqüência entre dois relógios (primeira derivada do *offset* no tempo).
Slot	Em um *HSM (Hardware Security Module)*, um *slot* é um leitor lógico que pontencialmente contém um *token.*
Smart Card	i. É um tipo de cartão plástico semelhante a um cartão de crédito com um ou mais *microchips* embutidos, capaz de armazenar e processar dados. Um *smart card* pode ser programado para desempenhar

PALAVRA CHAVE	DESCRIÇÃO
	inúmeras funções, inclusive pode ter capacidade de gerar chaves públicas e privadas e de armazenar certificados digitais. Pode ser utilizado tanto para controle de acesso lógico como para controle de acesso físico. ii. Um pequeno dispositivo, geralmente do tamanho de um cartão de crédito, que contém um processador e é capaz de armazenar informação criptográfica (como chaves e certificado) e realizar operações criptográficas.
S/MIME (Secure / Multipurpose Internet Mail Extensions)	Protocolo de segurança de *e-mail*. Foi desenhado para prevenir a interceptação e falsificação de *e-mail* usando cifração e assinatura digital. S/MIME constrói a segurança em cima do protocolo MIME e é baseado na tecnologia desenvolvida originalmente pela *RSA Data Security, Inc.*
SO	i. Sistema Operacional; ii. Em um *HSM (Hardware Security Module)*, é o *Security Officer,* é um usuário do dispositivo criptográfico com poderes de administrador do sistema.
Software	i. Programa de computador que utiliza uma seqüência lógica de instruções que o computador é capaz de executar para obter um resultado específico. ii. Conjunto de programas e instruções que operam o computador. São dois os tipos de *software* de computador: *software* de sistema, o qual engloba operações básicas necessárias para operar o *hardware* (por exemplo, sistema operacional, utilitários de comunicação, monitores de performance, editores, compiladores etc.) e *software* aplicativo, o qual executa tarefas específicas para auxiliar os usuários em suas atividades. iii. Programas e componentes de dados que podem ser dinamicamente modificados durante a execução, usualmente armazenados em mídias regraváveis.
SSL (Secure Socket Layer)	Protocolo de segurança que fornece privacidade na comunicação através da internet. É orientado a conexão, com serviço de crifração ponto-a-ponto possibilitando que aplicativos cliente(normalmente um navegador WEB) e servidore se comuniquem utilizando mecanismos criados para proteger o sigilo e a integridade do conteúdo, opcionalmente pode fornecer serviço de autenticação para entidades de camadas. Desenvolvido pela Netscape para transmitir documentos privativos pela internet.
Subscritor	Pessoa física ou jurídica que solicita os serviços de uma Autoridade de

PALAVRA CHAVE	DESCRIÇÃO
	Carimbo do Tempo (ACT), implícita ou explicitamente concordando com os termos mediante os quais o serviço é oferecido.
Suíte de Assinatura	Combinação de um esquema de assinatura com um método de padding e uma função resumo.
Suspensão de Certificado	Suspensão do uso de um certificado digital por um período determinado de tempo. A suspensão de certificado digital não é permitida no âmbito da ICP-Brasil.
Switch	Dispositivo que direciona pacotes em uma rede.
Template	Na especificação do *PKCS#11 (Cryptoki),* um *template* é um vetor de atributos e é usado para criar, manipular e procurar objetos.
TRC (Teorema de Resto Chinês)	Algoritmo, utilizado para resolver sistemas de congruências lineares, é muito antigo e foi inventado, independentemente, pelos chineses e pelos gregos, para resolver problemas de astronomia. O algoritmo chinês do resto tem este nome porque um dos primeiros lugares em que aparece é o livro *Manual de aritmética do mestre Sun*, escrito entre 287 d.C. e 473 d.C.
Tempo Universal Coordenado (UTC)	Escala de tempo adotada como padrão de Tempo Oficial Internacional, utilizada pelo sistema de Metrologia Internacional, Convenção do Metro, determinada e disseminada pelo *Bureau International des Poids et Mesures* - BIPM, França.
Terceira Parte (Relying Part)	i. Parte que age confiante no teor, validade e aplicabilidade do certificado digital e/ou carimbo do tempo emitido por uma das AC e/ ou ACT integrante da ICP-Brasil. ii. Pessoa ou instituição que age com total independência de fabricantes, desenvolvedores, representantes comerciais, prestadores de serviços de certificação digital e de potenciais compradores de sistemas e equipamentos de certificação digital
Termo de Responsabilidade	Termo assinado por uma pessoa física, que será a responsável pelo uso do certificado, quando o titular do certificado é uma organização. No termo, estão estabelecidas as condições de uso do certificado.
Termo de Titularidade	Termo assinado pelo titular do certificado digital emitido para pessoa física ou jurídica onde são estabelecidas as condições de uso do mesmo.
Termo Inicial de Fiscalização (TIF)	O documento que inicia o procedimento de fiscalização.

PALAVRA CHAVE	DESCRIÇÃO
Texto Cifrado	Dado que foi criptografado. O texto cifrado é a saída do processo de criptografia e pode ser transformado novamente em informação legível em forma de texto claro a partir da chave de decifração.
Texto Claro	Dado que está no estado não cifrado ou decifrado.
Thread-safe	Conceito de programação de computador aplicado ao contexto de programas *multi-threaded*. Uma parte do código é t*hread-safe* se funcionar corretamente durante a execução simultânea para *threads* múltiplas. Em particular, deve satisfazer à necessidade para *threads* múltiplas para acessar os mesmos dados compartilhados e a necessidade para uma parte compartilhada dos dados ser acessada por somente uma *thread* de cada vez.
Time-stamping	Vide Datação de Registros
Tipo de Certificados	Na ICP-Brasil estão definidos oito (08) tipos de certificados para titulares, classificados da seguinte forma: A1, A2, A3, A4, S1, S2, S3 e S4 e um tipo de certificado para Autoridades Certificadoras.
Titular de Certificado	Entidades, pessoa física ou jurídica, para as quais foram emitidos um certificado digital. O assinante é o titular da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra.
Token	i. Dispositivo para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o *smart card,* tendo sua conexão com o computador via USB. ii. Em um *HSM (Hardware Security Module),* um *token* é a visão lógica de um dispositivo criptográfico definido em *PKCS#11 (Cryptoki).*
Topologia	Disposição física dos nós e dos meios de rede dentro de uma estrutura de rede corporativa.
Transporte de Chaves (K*ey Transport*)	Processo ou protocolo que possibilita que uma chave criptográfica simétrica compartilhada seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.
Trilhas de Auditoria	i. Histórico das transações de sistemas que estão disponíveis para a avaliação com o objetivo de provar a correção de sua execução comparada com os procedimentos ditados pela política de segurança. ii. Rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria.

PALAVRA CHAVE	DESCRIÇÃO
	iii. Conjunto cronológico de registros que proporcionam evidências do funcionamento do sistema. Estes registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para rastrear o uso do sistema, detectando e identificando usuários não autorizados.
Triple DES (3DES)	Variação do DES, utilizando-o em três ciframentos sucessivos, podendo empregar uma versão com duas ou com três chaves diferentes. Seu tamanho de chave é de 112 ou 168 bits.
Unidade de Dado	No contexto da norma ISO 7816-4 representa o menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].
URL (Uniform Resource Locator)	Um mecanismo padronizado para identificar e localizar certos cadastros e outros recursos localizados na *World Wide Web*. A maioria das URLs aparece na forma familiar de endereços de sites.
Usuário	i. Pessoa que utiliza certificado digital apresentado por um titular. ii. Papel de acesso que quando assumido por uma entidade usuária externa permite realizar serviços de segurança no módulo criptográfico após sua iniciação, incluindo operações criptográficas, geração de chaves criptográficas, o uso do sistema de arquivos, sobrescrita do valor de chaves criptográficas (*key zeroization*), etc.
Usuário Final	Pessoa física ou jurídica que possui um certificado digital. Sinônimo de Titular de Certificado.
Validação da Cadeia de Certificados	Consiste na verificação da validade do certificado, nomeadamente a data, assinatura e validade dos certificados que estejam na sua cadeia de certificação, até ao certificado de confiança.
Validade de LCR	Período de tempo em que a LCR está com sua data de validade operacional. As LCR possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.
Validade do Certificado	Período de tempo em que o certificado está com sua data de validade operacional. Os Certificados possuem prazo máximo de validade de acordo com o tipo de certificado previsto na ICP-Brasil.
Verificação	Ratificação da identidade de uma pessoa física ou jurídica mediante a solicitação de certificado através de documentação apresentada pelo solicitante e da reconfirmação dos dados da solicitação.
Verificação da Validade do	Processo realizado por um destinatário ou terceira parte para confirmar que o certificado de um titular, usuário final, é válido e era operacional

PALAVRA CHAVE	DESCRIÇÃO
Certificado	na data e hora que uma assinatura digital pertinente foi criada.
Verificação de Assinatura digital	Ação realizada para determinar com precisão que: i. a assinatura digital foi criada durante o período operacional de um certificado válido por uma chave privada correspondente à chave pública contida no certificado e ii. que a mensagem associada não tenha sido alterada desde que a assinatura digital foi criada.
Vírus	Pequenos segmentos de códigos programados, normalmente com más intenções, que têm a característica de se agregar ao código de outros programas. Assim que são executados, disparam o código maliciosamente alterado a fim de causar modificações indevidas no processamento normal do sistema em que este se encontra, causando (ou não) desde danos leves a irreparáveis.
VPN (Virtual Private Networks)	Canal criptografado de dados que utiliza rede compartilhada de maneira segura. Os nós são conectados por meio de recursos de uma rede pública de telecomunicações, utilizando criptografia e outros dispositivos de segurança para garantir que os dados dessa rede não serão interceptados.
Vulnerabilidade	Fragilidade em uma máquina, programa ou sistema que pode ser explorada por um agressor. Agressores procuram por essas vulnerabilidades para explorá-las como forma de tomar acesso ao sistema. Um bom administrador de redes se mantém informado e atualizado de todas as vulnerabilidades descobertas nos sistemas, para agir de forma rápida na correção daquelas que dizem respeito ao ambiente que administra.
Worms	Programas maliciosos semelhantes aos vírus, porém se diferenciam na forma de infecção e nos tipos de danos que podem causar.
X.509	Recomendação ITU-T, a especificação X.509 é um padrão que especifica o formato dos certificados digitais, de tal maneira que se possa amarrar firmemente um nome a uma chave pública, permitindo autenticação forte. Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseadas em nomes distintos para localização. Na ICP-Brasil utilizam-se certificados no padrão X-509 V3.
Zeramento de Chaves	Vide *Key Zeroization*

ANEXO 6

DEMONSTRAÇÕES CONTÁBEIS

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	1

TITULO	BALANÇO PATRIMONIAL - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

ATIVO			PASSIVO		
ESPECIFICAÇÃO	**2017**	**2016**	ESPECIFICAÇÃO	**2017**	**2016**
ATIVO CIRCULANTE	**4.554.785,85**	**3.773.569,25**	**PASSIVO CIRCULANTE**	**-**	**-**
Caixa e Equivalentes de Caixa	**3.187.747,68**	**2.593.692,25**	**Obrigações Trabalh., Previd. e Assist. a Pagar a Curto Prazo**	**-**	**-**
Créditos a Curto Prazo	**-**	**-**	**Empréstimos e Financiamentos a Curto Prazo**	**-**	**-**
Demais Créditos e Valores a Curto Prazo	**1.193.698,76**	**972.606,90**	**Fornecedores e Contas a Pagar a Curto Prazo**	**-**	**-**
Investimentos e Aplicações Temporárias a Curto Prazo	**-**	**-**	**Obrigações Fiscais a Curto Prazo**	**-**	**-**
Estoques	**173.339,41**	**207.270,10**	**Obrigações de Repartição a Outros Entes**	**-**	**-**
VPDs Pagas Antecipadamente	**-**	**-**	**Provisões a Curto Prazo**	**-**	**-**
Ativos Não Financeiros Mantidos para Venda	**-**	**-**	**Demais Obrigações a Curto Prazo**	**-**	**-**
ATIVO NÃO CIRCULANTE	**8.904.960,32**	**9.895.449,02**	**PASSIVO NÃO CIRCULANTE**	**-**	**-**
Ativo Realizável a Longo Prazo	**-**	**-**	**Obrigações Trabalh., Previd. e Assist. a Pag. de Longo Prazo**	**-**	**-**
Estoques	-		**Empréstimos e Financiamentos a Longo Prazo**	**-**	**-**
Investimentos	**-**	**-**	**Fornecedores e Contas a Pagar a Longo Prazo**	**-**	**-**
Participações Permanentes	-	-	**Obrigações Fiscais a Longo Prazo**	**-**	**-**
Propriedades para Investimento	-	-	**Provisões a Longo Prazo**	**-**	**-**
Propriedades para Investimento	-	-	**Demais Obrigações a Longo Prazo**	**-**	**-**
(-) Depreciação Acumulada de Propriedades p/ Investimentos	-	-	**Resultado Diferido**	**-**	**-**
(-) Redução ao Valor Rec. de Propriedades para Investimentos	-	-	**TOTAL DO PASSIVO EXIGÍVEL**	**-**	**-**
Investimentos do RPSS de Longo Prazo	-	-	-		
Investimentos do RPSS de Longo Prazo	-	-	ESPECIFICAÇÃO	2017	2016
(-) Redução ao Valor Recuperável de Investimentos do RPPS	-	-	**Patrimônio Social e Capital Social**	**-**	**-**
Demais Investimentos Permanentes	-	-	**Adiantamentos para Futuro Aumento de Capital (AFAC)**	**-**	**-**
Demais Investimentos Permanentes	-	-	**Reservas de Capital**	**-**	**-**
(-) Redução ao Valor Recuperável de Demais Invest. Perm.	-	-	**Ajustes de Avaliação Patrimonial**	**-**	**-**
Imobilizado	**8.904.960,32**	**9.895.449,02**	**Reservas de Lucros**	**-**	**-**
Bens Móveis	5.454.620,32	6.445.109,02	**Demais Reservas**	**-**	**-**
Bens Móveis	12.532.846,31	12.257.831,94	**Resultados Acumulados**	**13.459.746,17**	**13.669.018,27**
(-) Depreciação/Amortização/Exaustão Acum. de Bens Móveis	-7.078.225,99	-5.812.722,92	Resultado do Exercício	-474.682,10	29.867,98
(-) Redução ao Valor Recuperável de Bens Móveis	-	-	Resultados de Exercícios Anteriores	13.669.018,27	13.639.150,29
Bens Imóveis	3.450.340,00	3.450.340,00	Ajustes de Exercícios Anteriores	265.410,00	
Bens Imóveis	3.450.340,00	3.450.340,00	**(-) Ações / Cotas em Tesouraria**	**-**	**-**
(-) Depr./Amortização/Exaustão Acum. de Bens Imóveis	-	-	**TOTAL DO PATRIMÔNIO LÍQUIDO**	**13.459.746,17**	**13.669.018,27**
(-) Redução ao Valor Recuperável de Bens Imóveis	-	-			
Intangível	**-**	**-**			
Softwares	-	-			
Softwares	-	-			
(-) Amortização Acumulada de Softwares	-	-			
(-) Redução ao Valor Recuperável de Softwares	-	-			
Marcas, Direitos e Patentes Industriais	-	-			
Marcas, Direitos e Patentes Industriais	-	-			
(-) Amortização Acumulada de Marcas, Direitos e Patentes Ind	-	-			

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	PERIODO
2017	Anual

EMISSAO	PAGINA
02/02/2018	2

VALORES EM UNIDADES DE REAL

TITULO	BALANÇO PATRIMONIAL - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

ATIVO			PASSIVO		
ESPECIFICAÇÃO	**2017**	**2016**	-		
			ESPECIFICAÇÃO	2017	2016
(-) Redução ao Valor Recuperável de Marcas, Direitos e Pat.	-	-			
Direitos de Uso de Imóveis	-	-			
Direitos de Uso de Imóveis	-	-			
(-) Amortização Acumulada de Direito de Uso de Imóveis	-	-			
(-) Redução ao Valor Recuperável Direito de Uso de Imóveis	-	-			
Diferido	**-**	**-**			
TOTAL DO ATIVO	**13.459.746,17**	**13.669.018,27**	**TOTAL DO PASSIVO E PATRIMÔNIO LÍQUIDO**	**13.459.746,17**	**13.669.018,27**

ATIVO			PASSIVO		
ESPECIFICAÇÃO	**2017**	**2016**	ESPECIFICAÇÃO	**2017**	**2016**
ATIVO FINANCEIRO	**3.187.747,68**	**2.593.692,25**	**PASSIVO FINANCEIRO**	**5.540.858,43**	**1.906.778,05**
ATIVO PERMANENTE	**10.271.998,49**	**11.075.326,02**	**PASSIVO PERMANENTE**	**-**	**-**
			SALDO PATRIMONIAL	**7.918.887,74**	**11.762.240,22**

Quadro de Compensações

ATIVO			PASSIVO		
ESPECIFICAÇÃO	**2017**	**2016**	ESPECIFICAÇÃO	**2017**	**2016**
ESPECIFICAÇÃO / Saldo dos Atos Potenciais Ativos			ESPECIFICAÇÃO / Saldo dos Atos Potenciais Passivos		
SALDO DOS ATOS POTENCIAIS ATIVOS	**2.153.802,85**	**1.997.614,49**	**SALDO DOS ATOS POTENCIAIS PASSIVOS**	**5.000.573,71**	**5.443.687,04**
Execução dos Atos Potenciais Ativos	2.153.802,85	1.997.614,49	Execução dos Atos Potenciais Passivos	5.000.573,71	5.443.687,04
Garantias e Contragarantias Recebidas a Executar	2.153.802,85	1.997.614,49	Garantias e Contragarantias Concedidas a Execut	-	-
Direitos Conveniados e Outros Instrumentos Cong	-	-	Obrigações Conveniadas e Outros Instrum Congên	-	-
Direitos Contratuais a Executar	-	-	Obrigações Contratuais a Executar	5.000.573,71	5.443.687,04
Outros Atos Potenciais Ativos a Executar	-	-	Outros Atos Potenciais Passivos a Executar	-	-
TOTAL	**2.153.802,85**	**1.997.614,49**	**TOTAL**	**5.000.573,71**	**5.443.687,04**

DEMONSTRATIVO DO SUPERÁVIT/DÉFICIT FINANCEIRO APURADO NO BALANÇO PATRIMONIAL

DESTINAÇÃO DE RECURSOS	SUPERAVIT/DEFICT FINANCEIRO
Recursos Ordinários	**-3.624.128,12**
Recursos Vinculados	**1.271.017,37**
Outros Recursos Vinculados a Órgãos e Programas	1.271.017,37
TOTAL	**-2.353.110,75**

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	1

TITULO	BALANÇO FINANCEIRO - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

INGRESSOS			DISPÊNDIOS		
ESPECIFICAÇÃO	**2017**	**2016**	ESPECIFICAÇÃO	**2017**	**2016**
Receitas Orçamentárias	**501.578,34**	**624.035,17**	**Despesas Orçamentárias**	**19.095.867,49**	**17.634.125,79**
Ordinárias	**1.086,34**	**1.304,92**	**Ordinárias**	**18.635.028,49**	**17.584.125,79**
Vinculadas	**500.492,00**	**622.730,25**	**Vinculadas**	**460.839,00**	**50.000,00**
Outros Recursos Vinculados a Órgãos e Programas	500.492,00	622.730,25	Outros Recursos Vinculados a Órgãos e Programas	460.839,00	50.000,00
(-) Deduções da Receita Orçamentária	-	-			
Transferências Financeiras Recebidas	**16.362.717,52**	**18.334.296,07**	**Transferências Financeiras Concedidas**	**1.307.186,22**	**1.276.554,34**
Resultantes da Execução Orçamentária	15.803.372,81	18.034.058,89	Resultantes da Execução Orçamentária	1.306.099,88	1.275.249,42
Repasse Recebido	15.803.372,81	18.034.058,89	Repasse Concedido	1.306.099,88	1.275.249,42
Independentes da Execução Orçamentária	559.344,71	300.237,18	Independentes da Execução Orçamentária	1.086,34	1.304,92
Transferências Recebidas para Pagamento de RP	559.344,71	300.237,18	Movimento de Saldos Patrimoniais	1.086,34	1.304,92
Aporte ao RPPS	-	-	Aporte ao RPPS	-	-
Aporte ao RGPS	-	-	Aporte ao RGPS	-	-
Recebimentos Extraorçamentários	**5.055.462,17**	**1.768.887,01**	**Despesas Extraorçamentárias**	**922.648,89**	**733.466,26**
Inscrição dos Restos a Pagar Processados	-	-	Pagamento dos Restos a Pagar Processados	-	-
Inscrição dos Restos a Pagar Não Processados	5.032.286,26	1.755.788,29	Pagamento dos Restos a Pagar Não Processados	899.472,98	697.637,29
Depósitos Restituíveis e Valores Vinculados	23.175,91	13.098,72	Depósitos Restituíveis e Valores Vinculados	23.175,91	35.828,97
Outros Recebimentos Extraorçamentários	-	-	Outros Pagamentos Extraorçamentários	-	-
Saldo do Exercício Anterior	**2.593.692,25**	**1.510.620,39**	**Saldo para o Exercício Seguinte**	**3.187.747,68**	**2.593.692,25**
Caixa e Equivalentes de Caixa	2.593.692,25	1.510.620,39	Caixa e Equivalentes de Caixa	3.187.747,68	2.593.692,25
TOTAL	**24.513.450,28**	**22.237.838,64**	**TOTAL**	**24.513.450,28**	**22.237.838,64**

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	1

TITULO	BALANÇO ORÇAMENTÁRIO - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

RECEITA

RECEITAS ORÇAMENTÁRIAS	PREVISÃO INICIAL	PREVISÃO ATUALIZADA	RECEITAS REALIZADAS	SALDO
RECEITAS CORRENTES	**460.839,00**	**460.839,00**	**501.578,34**	**40.739,34**
Receitas Tributárias	**-**	**-**	**-**	**-**
Impostos	-	-	-	-
Taxas	-	-	-	-
Contribuições de Melhoria	-	-	-	-
Receitas de Contribuições	**-**	**-**	**-**	**-**
Contribuições Sociais	-	-	-	-
Contribuições de Intervenção no Domínio Econômico	-	-	-	-
Cont. Entidades Privadas de Serviço Social Formação Profis.	-	-	-	-
Receita Patrimonial	**-**	**-**	**-**	**-**
Exploração do Patrimônio Imobiliário do Estado	-	-	-	-
Valores Mobiliários	-	-	-	-
Delegação de Serviços Públicos	-	-	-	-
Exploração de Recursos Naturais	-	-	-	-
Exploração do Patrimônio Intangível	-	-	-	-
Cessão de Direitos	-	-	-	-
Demais Receitas Patrimoniais	-	-	-	-
Receita Agropecuária	**-**	**-**	**-**	**-**
Receita Industrial	**-**	**-**	**-**	**-**
Receitas de Serviços	**460.839,00**	**460.839,00**	**500.492,00**	**39.653,00**
Serviços Administrativos e Comerciais Gerais	460.839,00	460.839,00	500.492,00	39.653,00
Serviços e Atividades Referentes à Navegação e ao Transporte	-	-	-	-
Serviços e Atividades Referentes à Saúde	-	-	-	-
Serviços e Atividades Financeiras	-	-	-	-
Outros Serviços	-	-	-	-
Transferências Correntes	**-**	**-**	**-**	**-**
Outras Receitas Correntes	**-**	**-**	**1.086,34**	**1.086,34**
Multas Administrativas, Contratuais e Judiciais	-	-	-	-
Indenizações, Restituições e Ressarcimentos	-	-	1.086,34	1.086,34
Bens, Direitos e Valores Incorporados ao Patrimônio Público	-	-	-	-
Demais Receitas Correntes	-	-	-	-
RECEITAS DE CAPITAL	**-**	**-**	**-**	**-**
Operações de Crédito	**-**	**-**	**-**	**-**
Operações de Crédito - Mercado Interno	-	-	-	-
Operações de Crédito - Mercado Externo	-	-	-	-
Alienação de Bens	**-**	**-**	**-**	**-**
Alienação de Bens Móveis	-	-	-	-
Alienação de Bens Imóveis	-	-	-	-
Alienação de Bens Intangíveis	-	-	-	-
Amortização de Empréstimos	**-**	**-**	**-**	**-**
Transferências de Capital	**-**	**-**	**-**	**-**
Outras Receitas de Capital	**-**	**-**	**-**	**-**

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	2

TITULO	BALANÇO ORÇAMENTÁRIO - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

RECEITA

RECEITAS ORÇAMENTÁRIAS	PREVISÃO INICIAL	PREVISÃO ATUALIZADA	RECEITAS REALIZADAS	SALDO
Integralização do Capital Social	-	-	-	-
Resultado do Banco Central do Brasil	-	-	-	-
Remuneração das Disponibilidades do Tesouro Nacional	-	-	-	-
Resgate de Títulos do Tesouro Nacional	-	-	-	-
Demais Receitas de Capital	-	-	-	-
RECURSOS ARRECADADOS EM EXERCÍCIOS ANTERIORES	**-**	**-**	**-**	**-**
SUBTOTAL DE RECEITAS	**460.839,00**	**460.839,00**	**501.578,34**	**40.739,34**
REFINANCIAMENTO	**-**	**-**	**-**	**-**
Operações de Crédito - Mercado Interno	**-**	**-**	**-**	**-**
Mobiliária	**-**	**-**	**-**	**-**
Contratual	**-**	**-**	**-**	**-**
Operações de Crédito - Mercado Externo	**-**	**-**	**-**	**-**
Mobiliária	**-**	**-**	**-**	**-**
Contratual	**-**	**-**	**-**	**-**
SUBTOTAL COM REFINANCIAMENTO	**460.839,00**	**460.839,00**	**501.578,34**	**40.739,34**
DEFICIT			**18.594.289,15**	**18.594.289,15**
TOTAL	**460.839,00**	**460.839,00**	**19.095.867,49**	**18.635.028,49**
DETALHAMENTO DOS AJUSTES NA PREVISÃO ATUALIZADA	**-**	**-**	**-**	**-**
Créditos Adicionais Abertos com Superávit Financeiro	-	-	-	-
Créditos Adicionais Abertos com Excesso de Arrecadação	-	-	-	-
Créditos Cancelados Líquidos	-	-	-	-
Créditos Adicionais Reabertos	-	-	-	-

DESPESA

DESPESAS ORÇAMENTÁRIAS	DOTAÇÃO INICIAL	DOTAÇÃO ATUALIZADA	DESPESAS EMPENHADAS	DESPESAS LIQUIDADAS	DESPESAS PAGAS	SALDO DA DOTAÇÃO
DESPESAS CORRENTES	**21.290.087,00**	**20.057.754,00**	**16.731.593,59**	**14.055.692,33**	**14.055.692,33**	**3.326.160,41**
Pessoal e Encargos Sociais	**7.291.543,00**	**7.317.566,00**	**5.485.421,86**	**4.543.080,25**	**4.543.080,25**	**1.832.144,14**
Juros e Encargos da Dívida	**-**	**-**	**-**	**-**	**-**	**-**
Outras Despesas Correntes	**13.998.544,00**	**12.740.188,00**	**11.246.171,73**	**9.512.612,08**	**9.512.612,08**	**1.494.016,27**
DESPESAS DE CAPITAL	**1.100.000,00**	**2.386.339,00**	**2.364.273,90**	**7.888,90**	**7.888,90**	**22.065,10**
Investimentos	**1.100.000,00**	**2.386.339,00**	**2.364.273,90**	**7.888,90**	**7.888,90**	**22.065,10**
Inversões Financeiras	**-**	**-**	**-**	**-**	**-**	**-**
Amortização da Dívida	**-**	**-**	**-**	**-**	**-**	**-**
RESERVA DE CONTINGÊNCIA	**-**	**-**	**-**	**-**	**-**	**-**
RESERVA DO RPPS	**-**	**-**	**-**	**-**	**-**	**-**
SUBTOTAL DAS DESPESAS	**22.390.087,00**	**22.444.093,00**	**19.095.867,49**	**14.063.581,23**	**14.063.581,23**	**3.348.225,51**
AMORTIZAÇÃO DA DÍVIDA / REFINANCIAMENTO	**-**	**-**	**-**	**-**	**-**	**-**
Amortização da Dívida Interna	**-**	**-**	**-**	**-**	**-**	**-**
Dívida Mobiliária	-	-	-	-	-	-
Outras Dívidas	-	-	-	-	-	-
Amortização da Dívida Externa	**-**	**-**	**-**	**-**	**-**	**-**
Dívida Mobiliária	-	-	-	-	-	-

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	PERIODO
2017	Anual

EMISSAO	PAGINA
02/02/2018	3

VALORES EM UNIDADES DE REAL

TITULO	BALANÇO ORÇAMENTÁRIO - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

DESPESA						
DESPESAS ORÇAMENTÁRIAS	DOTAÇÃO INICIAL	DOTAÇÃO ATUALIZADA	DESPESAS EMPENHADAS	DESPESAS LIQUIDADAS	DESPESAS PAGAS	SALDO DA DOTAÇÃO
Outras Dívidas	-	-	-	-	-	-
SUBTOTAL COM REFINANCIAMENTO	**22.390.087,00**	**22.444.093,00**	**19.095.867,49**	**14.063.581,23**	**14.063.581,23**	**3.348.225,51**
TOTAL	**22.390.087,00**	**22.444.093,00**	**19.095.867,49**	**14.063.581,23**	**14.063.581,23**	**3.348.225,51**

ANEXO 1 - DEMONSTRATIVO DE EXECUÇÃO DOS RESTOS A PAGAR NÃO PROCESSADOS

DESPESAS ORÇAMENTÁRIAS	INSCRITOS EM EXERCÍCIOS ANTERIORES	INSCRITOS EM 31 DE DEZEMBRO DO EXERCÍCIO ANTERIOR	LIQUIDADOS	PAGOS	CANCELADOS	SALDO
DESPESAS CORRENTES	**150.989,76**	**1.755.788,29**	**899.472,98**	**899.472,98**	**498.732,90**	**508.572,17**
Pessoal e Encargos Sociais	**-**	**654.248,52**	**234.403,10**	**234.403,10**	**419.845,42**	**-**
Juros e Encargos da Dívida	**-**	**-**	**-**	**-**	**-**	**-**
Outras Despesas Correntes	**150.989,76**	**1.101.539,77**	**665.069,88**	**665.069,88**	**78.887,48**	**508.572,17**
DESPESAS DE CAPITAL	**-**	**-**	**-**	**-**	**-**	**-**
Investimentos	**-**	**-**	**-**	**-**	**-**	**-**
Inversões Financeiras	**-**	**-**	**-**	**-**	**-**	**-**
Amortização da Dívida	**-**	**-**	**-**	**-**	**-**	**-**
TOTAL	**150.989,76**	**1.755.788,29**	**899.472,98**	**899.472,98**	**498.732,90**	**508.572,17**

ANEXO 2 - DEMONSTRATIVO DE EXECUÇÃO RESTOS A PAGAR PROCESSADOS E NAO PROCESSADOS LIQUIDADOS

DESPESAS ORÇAMENTÁRIAS	INSCRITOS EM EXERCÍCIOS ANTERIORES	INSCRITOS EM 31 DE DEZEMBRO DO EXERCÍCIO ANTERIOR	PAGOS	CANCELADOS	SALDO
DESPESAS CORRENTES	**-**	**-**	**-**	**-**	**-**
Pessoal e Encargos Sociais	**-**	**-**	**-**	**-**	**-**
Juros e Encargos da Dívida	**-**	**-**	**-**	**-**	**-**
Outras Despesas Correntes	**-**	**-**	**-**	**-**	**-**
DESPESAS DE CAPITAL	**-**	**-**	**-**	**-**	**-**
Investimentos	**-**	**-**	**-**	**-**	**-**
Inversões Financeiras	**-**	**-**	**-**	**-**	**-**
Amortização da Dívida	**-**	**-**	**-**	**-**	**-**
TOTAL	**-**	**-**	**-**	**-**	**-**

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

TITULO	DEMONSTRAÇÕES DAS VARIAÇÕES PATRIMONIAIS - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

EXERCICIO	PERIODO
2017	Anual
EMISSAO	**PAGINA**
02/02/2018	1

VALORES EM UNIDADES DE REAL

VARIAÇÕES PATRIMONIAIS QUANTITATIVAS

	2017	2016
VARIAÇÕES PATRIMONIAIS AUMENTATIVAS	**16.878.951,33**	**18.958.331,24**
Impostos, Taxas e Contribuições de Melhoria	**-**	**-**
Impostos	-	-
Taxas	-	-
Contribuições de Melhoria	-	-
Contribuições	**-**	**-**
Contribuições Sociais	-	-
Contribuições de Intervenção no Domínio Econômico	-	-
Contribuição de Iluminação Pública	-	-
Contribuições de Interesse das Categorias Profissionais	-	-
Exploração e Venda de Bens, Serviços e Direitos	**500.492,00**	**622.730,25**
Venda de Mercadorias	-	-
Vendas de Produtos	-	-
Exploração de Bens, Direitos e Prestação de Serviços	500.492,00	622.730,25
Variações Patrimoniais Aumentativas Financeiras	**-**	**-**
Juros e Encargos de Empréstimos e Financiamentos Concedidos	-	-
Juros e Encargos de Mora	-	-
Variações Monetárias e Cambiais	-	-
Descontos Financeiros Obtidos	-	-
Remuneração de Depósitos Bancários e Aplicações Financeiras	-	-
Aportes do Banco Central	-	-
Outras Variações Patr. Aumentativas Financeiras	-	-
Transferências e Delegações Recebidas	**16.364.432,99**	**18.334.296,07**
Transferências Intragovernamentais	16.362.717,52	18.334.296,07
Transferências Intergovernamentais	-	-
Transferências das Instituições Privadas	-	-
Transferências das Instituições Multigovernamentais	-	-
Transferências de Consórcios Públicos	-	-
Transferências do Exterior	-	-
Execução Orçamentária Delegada de Entes	-	-
Transferências de Pessoas Físicas	-	-
Outras Transferências e Delegações Recebidas	1.715,47	-
Valorização e Ganhos c/ Ativos e Desincorporação de Passivos	**12.940,00**	**-**
Reavaliação de Ativos	-	-
Ganhos com Alienação	-	-
Ganhos com Incorporação de Ativos	12.940,00	-
Ganhos com Desincorporação de Passivos	-	-
Reversão de Redução ao Valor Recuperável	-	-
Outras Variações Patrimoniais Aumentativas	**1.086,34**	**1.304,92**
Variação Patrimonial Aumentativa a Classificar	-	-
Resultado Positivo de Participações	-	-
Operações da Autoridade Monetária	-	-

MINISTÉRIO DA FAZENDA
SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	2

TITULO	DEMONSTRAÇÕES DAS VARIAÇÕES PATRIMONIAIS - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

VARIAÇÕES PATRIMONIAIS QUANTITATIVAS

	2017	2016
Reversão de Provisões e Ajustes para Perdas	-	-
Diversas Variações Patrimoniais Aumentativas	1.086,34	1.304,92
VARIAÇÕES PATRIMONIAIS DIMINUTIVAS	**17.353.633,43**	**18.928.463,26**
Pessoal e Encargos	**4.639.152,28**	**6.185.961,33**
Remuneração a Pessoal	2.160.559,11	1.991.201,12
Encargos Patronais	269.512,34	236.736,50
Benefícios a Pessoal	82.760,79	63.480,49
Outras Var. Patrimoniais Diminutivas - Pessoal e Encargos	2.126.320,04	3.894.543,22
Benefícios Previdenciários e Assistenciais	**-**	**-**
Aposentadorias e Reformas	-	-
Pensões	-	-
Benefícios de Prestação Continuada	-	-
Benefícios Eventuais	-	-
Políticas Públicas de Transferência de Renda	-	-
Outros Benefícios Previdenciários e Assistenciais	-	-
Uso de Bens, Serviços e Consumo de Capital Fixo	**11.339.425,17**	**11.422.398,31**
Uso de Material de Consumo	46.921,34	42.438,71
Serviços	10.026.657,06	10.095.594,40
Depreciação, Amortização e Exaustão	1.265.846,77	1.284.365,20
Variações Patrimoniais Diminutivas Financeiras	**-**	**-**
Juros e Encargos de Empréstimos e Financiamentos Obtidos	-	-
Juros e Encargos de Mora	-	-
Variações Monetárias e Cambiais	-	-
Descontos Financeiros Concedidos	-	-
Aportes ao Banco Central	-	-
Outras Variações Patrimoniais Diminutivas Financeiras	-	-
Transferências e Delegações Concedidas	**1.307.186,22**	**1.276.554,34**
Transferências Intragovernamentais	1.307.186,22	1.276.554,34
Transferências Intergovernamentais	-	-
Transferências a Instituições Privadas	-	-
Transferências a Instituições Multigovernamentais	-	-
Transferências a Consórcios Públicos	-	-
Transferências ao Exterior	-	-
Execução Orçamentária Delegada a Entes	-	-
Outras Transferências e Delegações Concedidas	-	-
Desvalorização e Perda de Ativos e Incorporação de Passivos	**12.596,30**	**-**
Reavaliação, Redução a Valor Recuperável e Ajustes p/ Perdas	-	-
Perdas com Alienação	-	-
Perdas Involuntárias	12.596,30	-
Incorporação de Passivos	-	-
Desincorporação de Ativos	-	-

MINISTÉRIO DA FAZENDA

SECRETARIA DO TESOURO NACIONAL

EXERCICIO	2017
PERIODO	Anual
EMISSAO	02/02/2018
PAGINA	3

TITULO	DEMONSTRAÇÕES DAS VARIAÇÕES PATRIMONIAIS - TODOS OS ORÇAMENTOS
SUBTITULO	24208 - INSTITUTO NAC.DE TECNOLOGIA DA INFORMACAO-ITI - AUTARQUIA
ORGAO SUPERIOR	20101 - PRESIDENCIA DA REPUBLICA

VALORES EM UNIDADES DE REAL

VARIAÇÕES PATRIMONIAIS QUANTITATIVAS

	2017	2016
Tributárias	**54.496,16**	**43.549,28**
Impostos, Taxas e Contribuições de Melhoria	46.767,34	43.549,28
Contribuições	7.728,82	-
Custo - Mercadorias, Produtos Vend. e dos Serviços Prestados	**-**	**-**
Custo das Mercadorias Vendidas	-	-
Custos dos Produtos Vendidos	-	-
Custo dos Serviços Prestados	-	-
Outras Variações Patrimoniais Diminutivas	**777,30**	**-**
Premiações	-	-
Resultado Negativo de Participações	-	-
Operações da Autoridade Monetária	-	-
Incentivos	-	-
Subvenções Econômicas	-	-
Participações e Contribuições	-	-
Constituição de Provisões	-	-
Diversas Variações Patrimoniais Diminutivas	777,30	-
RESULTADO PATRIMONIAL DO PERÍODO	**-474.682,10**	**29.867,98**

VARIAÇÕES PATRIMONIAIS QUALITATIVAS

	2017	2016