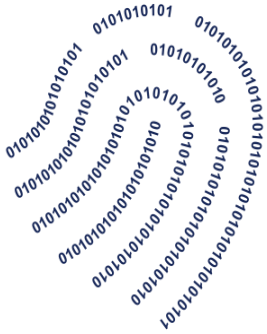
PLANO DE INTEGRIDADE E COMPLIANCE



Instituto Nacional de Tecnologia da Informação

PRESIDÊNCIA DA REPÚBLICA – CASA CIVIL
SCN Quadra 02 Bloco E – CEP 70712-905 – BRASÍLIA/DF
Telefone: (61) 3424-3875 – https://www.iti.gov.br

MARÇO – 2019

ITI – Instituto Nacional de Tecnologia da Informação

SCN Quadra 02 Bloco E CEP 70712-905 Brasília/DF

https://www.iti.gov.br

Marcelo Amaro Buz

Diretor-Presidente

Waldeck Araújo Jr.

Diretor de Infraestrutura de Chaves Públicas

Ângela Maria de Oliveira

Diretora de Auditoria, Fiscalização e Normalização

Ronoilton Gonçalves

Coordenador-Geral de Planejamento, Orçamento e Administração

Brasília/2019

DECLARAÇÃO DA ALTA ADMINISTRAÇÃO

"Sem integridade, rompe-se a ética empresarial e rompe-se a governança corporativa"

Apresentamos o Plano de Integridade e Compliance do Instituto Nacional de Tecnologia da Informação – ITI aos nossos colaboradores e à sociedade.

O ITI por intermédio do Plano de Integridade e Compliance objetiva implantar a prática de valores éticos e morais, prezando pela transparência, imparcialidade, lisura nas relações entre servidores, excelência na prestação dos serviços e sempre alinhado com o que preconiza o Planejamento Estratégico 2019-2022.

Acreditamos que tais práticas fluirão naturalmente se adotadas como cultura da autarquia, eliminando quaisquer possibilidades de vícios, fraudes e atos de corrupção. Destarte, o engajamento de todos os líderes, servidores, fornecedores, estagiários, terceirizados, colaboradores e cidadãos é condição essencial para que o enraizamento dos valores que compõem o SER ÍNTEGRO (probo, irrepreensível na sua conduta, honesto, incorruptível) prevaleça sem necessidade de ser impositivo.

Confiantes que o Plano de Integridade e Compliance da ITI será um valioso guia para respaldar a atitude de todos, construindo uma empresa que possa solidificar a integridade nas relações humanas e nos seus negócios, subscrevemo-nos.

Marcelo Amaro Buz
Diretor-Presidente

Waldeck Araújo Jr.
Diretor de Infraestrutura de Chaves Públicas

Ângela Maria de Oliveira
Diretora de Auditoria, Fiscalização e Normalização

Ronoilton Gonçalves
Coordenador-Geral de Planejamento, Orçamento e Administração

SUMÁRIO

1. INFORMAÇÕES SOBRE A INSTITUIÇÃO

O INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO – ITI é uma autarquia federal criada pela Medida Provisória n. 2.200-2, de 24 de agosto de 2001, com sede e foro no Distrito Federal, vinculada à Casa Civil da Presidência da República e tem como escopo manter e executar as políticas da Infraestrutura de Chaves Públicas Brasileira – ICP/Brasil.

O ITI, como Autoridade Certificadora Raiz da ICP – Brasil (AC-RAIZ), é a primeira autoridade da cadeia de certificação e a ele compete emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu, seguindo as políticas de certificados e normas técnicas operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, instituído pelo Decreto 6.605, de 14 de outubro de 2008.

1.1 PRINCIPAIS COMPETÊNCIAS E SERVIÇOS PRESTADOS PELO ÓRGÃO

O ITI tem uma série de atribuições que o faz assegurar a realização do seu propósito. Elas serão elencadas abaixo em conformidade com o que preceitua o Regimento Interno do Órgão. Pode-se, entretanto, sintetizar como principais competências a execução das políticas de certificação, cumprimento das normas técnicas/operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, bem como a operacionalização, manutenção e modernização do sistema nacional de certificação digital.

A atuação do ITI, primeira Autoridade da Cadeia de Certificação Digital – AC Raiz e Entidade Raiz da Rede de Carimbo do Tempo da Infraestrutura de Chaves Públicas, com respaldo nos preceitos legais e regulamentares, desenvolve-se sob as seguintes competências:

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

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

III – gerencia os certificados da Autoridade Certificadora Raiz – AC RAIZ e das autoridades Certificadoras – AC de nível imediatamente inferior e lateral;

IV – provê a segurança física e lógica e a infraestrutura tecnológica da AC RAIZ e da Entidade de Auditoria do Tempo – EAT;

V - gerencia as listas de certificados emitidos, revogados e vencidos das ACs – Autoridades Certificadoras;

VI - executa as atividades de fiscalização e de auditoria das ACs – Autoridades Certificadoras, Autoridades de Registro – ARs, das Autoridades de Carimbo do Tempo – ACTs e dos Prestadores de Serviços credenciados e autorizados na ICP-Brasil;

VII – aplica sanções e penalidades na forma da legislação;

VIII – credencia as entidades previstas perante a ICP-Brasil;

IX – promove o relacionamento com instituições congêneres no país e no exterior;

X – celebra e acompanha 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;

XI – estimula a participação de universidades, instituições de ensino e iniciativa privada em pesquisa e desenvolvimento nas atividades de interesse da área da Autarquia;

XII – estimula e articula projetos de pesquisa científica e de desenvolvimento tecnológico, voltados à ampliação da cidadania digital, por meio de tecnologias que garantam a privacidade, a autenticidade e a integridade de informações eletrônicas;

XIII – presta o apoio técnico e administrativo à Secretaria-Executiva do Comitê Gestor da ICP-Brasil e

XIV – fomenta o uso de certificado digital e tecnologias associadas para toda a administração pública federal.

ENTES DA ICP-BRASIL

Publicado: Terça, 27 de Junho de 2017, 18h08 | Última atualização em Quinta, 05 de Abril de 2018, 14h23

AC - Raiz

A Autoridade Certificadora Raiz da ICP-Brasil – AC-Raiz é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil. Portanto, compete à AC-Raiz emitir, expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

A AC-Raiz também está encarregada de emitir a Lista de Certificados Revogados – LCR e de fiscalizar e auditar as Autoridades Certificadoras – ACs, Autoridades de Registro – ARs e demais prestadores de serviço habilitados na ICP-Brasil. Como também, de verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da 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 assinante, 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 de Registro – 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 – AC. Vinculada a uma AC, tem por objetivo o recebimento, a validação, o 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 emissão dos mesmos. 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 seu conteúdo é criptografado. 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. A ACT atesta não apenas a questão temporal de uma transação, mas também seu conteúdo.

PSS - Prestador de Serviço de Suporte

O PSS desempenha atividade descrita nas Políticas de Certificado - PC e na Declaração de Práticas de Certificação - DPC da AC a que estiver vinculado, diretamente ou por intermédio da AR, ou nas Políticas de Carimbo do Tempo - PCT e na Declaração de Práticas de Carimbo do Tempo - DPCT da ACT a que estiver vinculado, ou ainda nas atividades de PSBio, classificando-se, conforme o tipo de atividade prestada, em três categorias: disponibilização de infraestrutura física e lógica; disponibilização de recursos humanos especializados; ou disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

PSBio - Prestador de Serviço Biométrico

Os PSBios são entidades com capacidade técnica para realizar a identificação biométrica, tornando um registro/requerente único em um ou mais bancos/sistemas de dados biométricos para toda ICP-Brasil, a verificação biométrica do requerente de um certificado digital e a comparação de uma biometria, que possua característica perene e unívoca, de acordo com os padrões internacionais de uso.

Eis abaixo, como exemplificação, as Autoridades Certificadoras – ACs de 1º nível da ICP – Brasil já credenciadas pelo ITI.

Relação de Autoridades Certificadoras de 1º nível da ICP-Brasil:

1 – SERPRO – Serviço Federal de Processamento de Dados

2 – Caixa Econômica Federal

3 – SERASA Experian

4 – Receita Federal do Brasil

5 – CERTISIGN

6 – Imprensa Oficial do Estado de São Paulo

7 – AC JUS – Autoridade Certificadora da Justiça Federal

8 – AC PR – Autoridade Certificadora da Presidência da República

9 – Casa da Moeda do Brasil

10 – VALID Certificadora Digital

11 - SOLUTI Certificação Digital

12 – AC Digitalsign

13 – AC Boa Vista

14 – Ministério das Relações Exteriores

15 – AC Defesa – Ministério da Defesa

16 – AC Safeweb

17 – PRODEMGE - Companhia de Tecnologia da Informação do Estado de Minas Gerais

Obs: A estrutura da ICP-Brasil, atualizada até 07.02.2019, está publicada no site da ITI (www.iti.gov.br), com todas as autoridades certificadoras de 1º e 2º níveis.

1.2 ESTRUTURA REGIMENTAL

O Decreto nº 8.985, de 8 de fevereiro de 2017, alterado pelo Decreto n. 9.183, de 30 de outubro de 2017, aprovou a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Instituto Nacional de Tecnologia da Informação – ITI.

A Portaria n. 20, de 28 de fevereiro de 2018, aprovou o Regimento Interno do Instituto Nacional de Tecnologia da Informação – ITI. Assim, todas as informações sobre a estrutura organizacional e respectivas competências do referido Órgão estão contidas neste instrumento normativo. Entretanto, para se ter uma visão do arcabouço que dá sustentação e funcionamento ao ITI, transcreveu-se a seguir sua estrutura organizacional:

I - Órgãos de assistência direta e imediata ao Diretor-Presidente:

a) Gabinete - GABIN;

1. Assessoria de Comunicação - ASCOM;

b) Assessoria Especial - ASESP;

c) Coordenação de Auditoria Interna - COAUD e

d) Procuradoria Federal Especializada - PFESP.

II - Órgão seccional:

a) Coordenação-Geral de Planejamento, Orçamento e Administração - CGPOA:

1. Coordenação de Execução Orçamentária e Financeira - COEFI;

2. Coordenação de Licitações, Contratos e Convênios - COLIC;

3. Coordenação de Planejamento, Orçamento e Modernização Institucional - COPOM;

4. Divisão de Recursos Logísticos - DILOG;

5. Serviço de Contabilidade – SECON e

6. Serviço de Gestão de Pessoas - SEGEP.

III - Órgãos específicos singulares:

a) Diretoria de Infraestrutura de Chaves Públicas - DINFRA:

1- Coordenação de Tecnologia da Informação e Comunicações – COTIC;

2. Coordenação-Geral de Infraestrutura e Segurança da Informação – CGISI:

2.1. Coordenação de Segurança da Informação – COSIN e

2.2. Coordenação de Infraestrutura Tecnológica – COTEC.

3. Coordenação-Geral de Operações – CGOPE e

3.1. Coordenação de Operação da AC Raiz – COACR.

b) Diretoria de Auditoria, Fiscalização e Normalização - DAFN:

1. Coordenação-Geral de Auditoria e Fiscalização - CGAFI e

2. Coordenação-Geral de Normalização e Pesquisa - CGNPE.

1.3 SETOR DE ATUAÇÃO E PRINCIPAIS PARCERIAS

A Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz – AC-Raiz, também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Vale a pena citar aqui a importância e presença do ITI na desburocratização e celeridade de atividades do cotidiano dos cidadãos brasileiros:

Publicado: Quinta, 29 de Junho de 2017, 13h25 | Última atualização em Quinta, 26 de Abril de 2018, 15h40.

O certificado digital facilita o acesso a diversos serviços pela internet. Confira alguns dos programas e sistemas que devem ser acessados com certificado digital ICP-Brasil e outras iniciativas que fazem uso da tecnologia:

Atendimento Virtual - e-CAC: sistema da Receita Federal que possui diversos serviços protegidos por sigilo fiscal, que podem ser acessados pelo usuário com certificado digital. Por meio do e-CAC podem ser realizadas ações como verificação de pendências na declaração do Imposto de enda, obtenção de cópia de declarações, retificação de pagamentos, parcelamento de débitos, pesquisas de situação fiscal e impressão de comprovantes. Na **página da Receita Federal** é possível conferir todos os serviços disponibilizados no e-CAC;

Bacenjud: sistema acessado com certificado digital que interliga a Justiça ao Banco Central e às instituição bancárias, para agilizar a solicitação de informações e o envio de ordens judiciais ao Sistema Financeiro Nacional, via internet;

Carteiras de Identidade Profissional: os advogados, médicos, corretores e contadores possuem carteiras de identidades profissionais, emitidas pelos respectivos órgãos de classe, com certificado digital, o que permite a esses profissionais a execução de inúmeras atividades com segurança e sem a necessidade de se deslocar fisicamente;

CNH Digital: a Carteira Nacional de Habilitação – CNH em formato digital foi aprovada pelo Contran em 2017. O documento eletrônico tem a mesma validade do documento impresso, visto que é assinado com certificado digital ICP-Brasil. A CNH digital pode ser apresentada em aparelhos eletrônicos, como *smartphones* e *tablets*, aos agentes de trânsito, que verificarão a autenticidade do documento através da leitura do QR-*Code* apresentado. Confira as instruções para emissão da CNH Digital no site do Denatran;

Conectividade Social ICP: canal eletrônico de relacionamento para troca de informações referentes ao FGTS entre a Caixa Econômica Federal, agente operador do fundo, e as empresas, escritórios de contabilidade, sindicatos, prefeituras e outros entes, deve ser acessado com certificado digital;

Decom Digital: sistema do MDIC para formação de autos digitais que permite o envio eletrônico de documentos no âmbito de petições e de processos de defesa comercial, bem como a visualização desses documentos a qualquer momento. O acesso e a assinatura de documentos no Decom é feito com certificado digital;

Diário Oficial da União – DOU: o documento passou a ser publicado no Portal da Imprensa Nacional assinado com certificado digital ICP-Brasil em agosto de 2009. A assinatura digital garante a segurança e a autenticidade das informações publicadas. Os Diários Oficiais da União assinados eletronicamente e disponibilizados no Portal da Imprensa Nacional são acessados aproximadamente 5 milhões de vezes por mês e 60 milhões de vezes por ano;

Documento de Origem Florestal – DOF: licença obrigatória emitida pelo Ibama para o controle do transporte de produto e subproduto florestal de origem nativa, inclusive o carvão vegetal nativo, no Brasil. O documento deve ser assinado digitalmente;

DMED: programa gerador da Declaração de Serviços Médicos e de Saúde - DMED que deve ser entregue a Receita Federal. A DMED deve ser assinado digitalmente com certificado digital;

e-RPC: os registros para programas de computador junto ao Instituto Nacional da Propriedade Industrial – INPI podem ser obtidos digitalmente por meio do Sistema On-line para Registro de Programas de Computador – e-RPC. Para fazer o pedido de registro, o usuário não precisa mais enviar o código-fonte do software para o INPI. Agora basta criptografá-lo na forma de resumo digital hash, garantindo assim o sigilo da informação. Esse resumo será transcrito no formulário eletrônico de depósito. O usuário anexará ao pedido a Declaração de Veracidade – DV, que deve ser assinada com certificado digital ICP-Brasil;

Escritório Digital: integra os sistemas processuais dos tribunais brasileiros e permiti ao usuário centralizar em um único endereço eletrônico a tramitação dos processos de seu interesse no Judiciário. O acesso ao sistema é feito com certificado digital;

eSocial: por meio do sistema, acessado com certificado digital, empregadores devem comunicar ao Governo, de forma unificada, as informações relativas aos trabalhadores, como vínculos, contribuições previdenciárias, folha de pagamento,

comunicações de acidente de trabalho, aviso prévio, escriturações fiscais e informações sobre o FGTS;

Inquérito Policial Eletrônico**:** o sistema elimina a tramitação de procedimentos em meio físico, tendo em vista que não há necessidade de impressão de documentos e assinatura de próprio punho. Segundo as autoridades policiais, com a redução da burocracia, os agentes poderão se dedicar mais à investigação e outras tarefas finalísticas. O certificado digital ICP-Brasil é utilizado no sistema que realiza a integração de dados entre a Polícia Civil e o Tribunal de Justiça.

MigranteWeb: sistema para autorizações de trabalho estrangeiro no Brasil. O acesso é realizado com certificado digital;

Nota Fiscal Eletrônica - NF-e: o documento, que substitui a nota fiscal eletrônica em papel, é assinado com certificado ICP-Brasil;

Passaporte Eletrônico: o novo passaporte eletrônico, que começou a ser emitido a partir de dezembro de 2010 pela Polícia Federal e pela Casa da Moeda, tem validade de 10 anos e é assinado digitalmente com certificado digital ICP-Brasil. Com o novo passaporte, o Brasil passou a fazer parte do PKD, o Diretório de Chaves Públicas da ICAO - Organização Internacional de Aviação Civil, o que agilizará a verificação de autenticidade do passaporte brasileiro em postos de controle migratório no exterior e proporcionará maior segurança aos viajantes brasileiros;

Portal Brasil Cidadão: o portal permite o acesso a diversos serviços públicos digitais, sem que o cidadão precise se deslocar, permanecer em filas, imprimir ou autenticar documentos. O acesso ao sistema pode ser feito com certificado digital ICP-Brasil. Além de praticidade e agilidade para cidadãos e empresários, os serviços digitais reduzirão em até 97% o custo para o governo e eliminarão muitas das dificuldades enfrentadas atualmente no atendimento presencial;

Portal de Compras Governamentais – Comprasnet: no portal é possível realizar processos eletrônicos de aquisições e disponibilizar informações referentes às licitações e contratações promovidas pelo Governo. Para acessar os diversos serviços do Comprasnet os fornecedores e pregoeiros devem adquirir um certificado digital ICP-Brasil;

Portal de indenizações de planos econômicos: Mais de um milhão de poupadores serão beneficiados com a correção de aplicações na poupança durante os planos econômicos Bresser (1987), Verão (1989) e Collor 2 (1991). Até abril de 2018, o portal unificado de pagamentos será disponibilizado pelos bancos onde os advogados responsáveis por cada ação poderão cadastrar-se, receber honorários e encaminhar os pagamentos de seus clientes. Para acesso ao sistema, será necessário o uso do certificado digital da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil;

Processo Judicial Eletrônico - PJ-e: sistema desenvolvido para automação do Judiciário, os acessos e as assinaturas das petições devem ser feitas com certificado digital. O objetivo principal é manter um sistema de processo judicial eletrônico capaz de permitir a prática de atos processuais, assim como o acompanhamento desse processo judicial, independentemente de o processo tramitar na Justiça Federal, na Justiça dos Estados, na Justiça Militar dos Estados e na Justiça do Trabalho;

Processo Judicial Eletrônico do Superior Tribunal de Justiça – e-STJ: sistema de peticionamento exclusivo do Superior Tribunal de Justiça, os acessos e as assinaturas das petições devem ser feitas com certificado digital;

Programa Cartão Reforma: iniciativa do Ministério das Cidades que beneficia famílias com renda mensal de até R$ 2.811 com recursos para compra de materiais de construção. O valor do benefício varia de R$ 2 mil a R$ 9 mil. As prefeituras e estados que têm interesse em participar do programa devem realizar a adesão com certificado digital ICP-Brasil;

Registrato: sistema administrado pelo Banco Central do Brasil que permite aos cidadãos terem acesso pela internet, de forma rápida e segura, a relatórios contendo informações sobre seus relacionamentos com as instituições financeiras e sobre suas operações de crédito. O acesso é facilitado para quem possui certificado digital;

SADIPEM: sistema do Tesouro Nacional para o envio e análise dos pleitos de operações de crédito dos entes federativos, o acesso ao sistema deve ser feito com certificado digital ICP-Brasil;

Simples Nacional: canal de acesso virtual, com certificado digital, à serviços referentes a tributos relacionados às Microempresas e Empresas de Pequeno Porte;

SICAF 100% Digital: a plataforma promete simplificar os procedimentos para cadastro no Sistema de Cadastramento Unificado de Fornecedores – SICAF. Até junho de 2018 todos fornecedores deverão adquirir certificado digital ICP-Brasil para participar das licitações do Governo Federal;

SISCOMEX: voltado aos operadores de comércio exterior - exportadores, importadores, transportadores, depositários, despachantes aduaneiros, terminais portuários, etc. - o Portal Siscomex facilita o acesso aos serviços e sistemas governamentais e à legislação pertinentes às operações de comércio exterior. O certificado ICP-Brasil é utilizado para autenticação no sistema e assinatura de documentos;

Serviço de Documentos Oficiais - SIDOF: tramitação de documentos oficiais entre os Ministérios e a Casa Civil da Presidência da República com uso do certificado digital, eliminando papel e dando celeridade ao processo;

Sistema de Concessão de Diárias e Passagens - SCDP: sistema eletrônico que integra as atividades de concessão, registro, acompanhamento, gestão e controle das diárias e passagens, decorrentes de viagens realizadas no interesse da administração, em território nacional ou estrangeiro. O sistema permite a tramitação eletrônica dos documentos com a utilização do certificado digital ICP-Brasil;

Sistema de Concessão Eletrônica de Isenção IPI/IOF – Sisen: taxistas podem requerer digitalmente a isenção de impostos, sem a necessidade de ir até um posto da Receita Federal. A solicitação deve ser feita por meio do Sistema de Concessão Eletrônica de Isenção IPI/IOF – SISEN. O acesso ao sistema pode ser realizado com certificado digital ICP-Brasil. O sistema também pode ser utilizado por pessoas com deficiência física, visual, mental severa/profunda ou autistas, no processo de aquisição de veículos com isenção do Imposto sobre Produtos Industrializados – IPI e do Imposto sobre Operações de Crédito, Câmbio e Seguro ou relativas a Títulos ou Valores Mobiliários – IOF.

Sistema de Gestão de Acesso – SIGAC: Todos os servidores, ativos e aposentados, e pensionistas do Governo Federal que precisam acessar documentos como: autorização de consignatária, contracheque, informe de rendimentos para Imposto de Renda, entre outros, podem encontrar essas informações no SIGAC, o acesso ao sistema pode ser feito de qualquer lugar com uso do certificado digital ICP-Brasil;

Sistema de Gestão Fundiária - SIGEF: sistema de gestão de informações fundiárias do meio rural brasileiro. Por ele são efetuadas a recepção, validação, organização, regularização e disponibilização das informações georreferenciadas de limites de imóveis rurais, todas as ações são realizadas com certificado ICP-Brasil;

Sistema de Pagamentos Brasileiro - SPB: gerencia o processo de compensação e liquidação de pagamentos por meio eletrônico, interligando 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 de Registro e Licenciamento de Empresas - RLE: integra a Administração Pública da União, dos estados e dos municípios, de forma a proporcionar, num processo único, simplificado, previsível e uniforme, a abertura, as licenças de funcionamento e, se for necessário, a baixa de empresas. No acesso com certificado digital há possibilidade de entrega de documentos digitais e assinatura digital de declarações e de outros documentos;

Sistema de Registro de Documentos dos Postos Revendedores: automatiza o atendimento a cerca de 40 mil postos de combustíveis atuantes no Brasil. Confere maior eficiência no contato com a ANP, ao reduzir custos e tempo, além de permitir o acompanhamento das solicitações feitas à ANP pela internet com uso do certificado digital ICP-Brasil;

Sistema Fisco Fácil: a Secretaria de Estado de Fazenda e Planejamento do estado do Rio de Janeiro lançou a ferramenta Fisco Fácil, que oferta serviços online de emissão de certidão negativa de débitos, baixa de inscrição estadual e consulta à malha fiscal. Para ter acesso aos serviços, que possibilitam ao contribuinte verificar e regularizar pendências, é obrigatório o uso do certificado digital ICP-Brasil;

Sistema Público de Escrituração Digital - Sped: a ferramenta da Receita Federal do Brasil possibilita o envio, com certificado digital, de informações de natureza fiscal e contábil para os órgãos de registro e para os fiscos das diversas esferas.

Vale salientar que a certificação digital ICP-Brasil está em um número incontável de sistemas que se converte em prestação direta de serviço ao cidadão, conforme acima exposto, sem que este precise comprar um certificado. O FGTS, a compensação de cheques por imagem, o Prontuário Eletrônico do Paciente, a tramitação totalmente eletrônica de processos judiciais,

os leilões da Receita Federal, entre outros, demonstram que a tecnologia democratizou o acesso da população a benefícios e direitos anteriormente morosos e complicados.

Na prática, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos, como a web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora (AC) que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

No que diz respeito a tecnologias auditáveis, a que está em uso atualmente na ICP-Brasil foi totalmente produzida no país por meio do programa João de Barro (pubicado no site:www.iti.gov.br), o que propicia total controle e auditoria por parte da Autoridade Certificadora Raiz, papel exercido pelo ITI.

É importante mencionar que entre meses de janeiro 2018 e dezembro de 2018, conforme informado no site (www.iti.gov.br), emitiu 4.416.398 de certificados digitais, no mesmo período de 2017, de janeiro a dezembro, foram emitidos 3.587.773. Houve crescimento de 23,10% de um ano para o outro.

O ITI tem eminente compromisso com a gestão pública eficiente, transparente e focada em resultados que caminhem ao encontro da construção da democracia e desburocratização por meio de ferramentas como o certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

Seguem transcritos a seguir, alguns exemplos de parcerias internacionais e nacionais firmadas pelo ITI:

PARCERIAS INTERNACIONAIS

Publicado: Quarta, 19 de abril de 2017, 10h51 | Última atualização em Terça, 31 de outubro de 2017, 10h20 (www.iti.gov.br)

Argentina - o uso do Certificado de Origem digital – COD, que reduzirá custos e prazos nas exportações entre Brasil e Argentina, entrará em vigência no dia 10 de maio. A divulgação da data ocorreu durante a quarta Reunião da Comissão Bilateral de Produção e Comércio em Buenos Aires, no começo deste mês, pelo ministro da Indústria, Comércio Exterior e Serviços

do Brasil, Marcos Pereira, e o ministro da Produção da Argentina, Francisco Cabrera. A assinatura digital do COD no Brasil se dará por meio do certificado digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.(...)

Publicado: Quinta, 29 de novembro de 2018, 13h29 | Última atualização em Quinta, 29 de novembro de 2018, 15h33 (www.iti.gov.br)

Honduras – (...)O ITI foi convidado a participar do importante momento para o governo de Honduras como parceiro no desenvolvimento de tecnologias e exemplo na América Latina de sucesso na implantação do uso da certificação digital, por meio da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. O diretor-presidente do ITI parabenizou o governo de Honduras pelo processo de modernização e colocou o Instituto à disposição para futuras parcerias e compartilhamento de experiências. (...)

Publicado: Quarta, 04 de novembro de 2015, 12h28 | Última atualização em Terça, 31 de outubro de 2017, 10h23

Teve início na manhã desta quarta-feira, 4 de novembro, uma série de encontros que vão até a próxima sexta-feira, 6, entre representantes do Instituto Nacional de Tecnologia da Informação – ITI, da *Smart Card Alliance* Latino America – SCALA e das Infraestruturas de Chaves Públicas da Costa Rica e do Peru. Os encontros, realizados na sede do ITI, em Brasília, têm por objetivo proporcionar debates sobre o cenário da certificação digital na região para aprimoramento no setor e possíveis parcerias internacionais. (...)

PARCERIAS NACIONAIS

Publicado: Quarta, 21 de março de 2018, 13h40 | Última atualização em Quarta, 21 de março de 2018, 13h40 (www.iti.gov.br)

Nos últimos dias 13 e 14 de março, o diretor-presidente do Instituto Nacional de Tecnologia da Informação – ITI Gastão José de Oliveira Ramos esteve na cidade do Rio de Janeiro para encontros com representantes de importantes entidades públicas. Como noticiado pelo ITI, o primeiro compromisso da agenda de trabalhos ocorreu no Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro, quando as instituições **assinaram Acordo de Cooperação**

Técnico-Científica com o objetivo de desenvolver ações e projetos cooperativos de pesquisa, desenvolvimento e inovação.

Após o ato, ainda no dia 13 houve reunião no Instituto Nacional de Propriedade Industrial – INPI. A instituição já faz uso da tecnologia ICP-Brasil no **Sistema Online para Registro de Programas de Computador – e-RPC** e pretende, em breve, fazer o mesmo **no registro de topografias de circuitos**. No dia 14 foi a vez de ir ao Banco Nacional do Desenvolvimento – BNDES para entendimentos sobre possíveis parcerias e uso de certificados ICP-Brasil.

"É muito importante que o ITI colabore para que entidades públicas façam do certificado ICP-Brasil o seu meio seguro de identificação e assinatura digital. Inmetro, INPI e BNDES são instituições renomadas, capazes de criar cases de repercussão nacional e que fazem interface com um incontável número de entes no Brasil e no exterior. Ao passo em que utilizem o certificado digital e obtenham êxito, poderão induzir outros ao mesmo, colaborando na disseminação e na massificação da tecnologia ICP-Brasil", comentou Gastão Ramos.

Na oportunidade, acompanharam o diretor-presidente seus assessores-técnicos Ruy Ramos, no dia 13, e José Antônio Carrijo, no dia 14.

Publicado: Quarta, 19 de agosto de 2015, 12h37 | Última atualização em Terça, 31 de outubro de 2017, 10h23

Foi assinado ontem, 17, na Universidade de Brasília – UnB, o Termo de Cooperação entre o Instituto Nacional de Tecnologia da Informação – ITI e a Fundação Universidade de Brasília – FUB/UnB, para pesquisa e desenvolvimento de um aplicativo que possibilitará a criação e verificação de assinaturas digital em arquivos PDF, baseadas no padrão de assinatura PADES da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

1.4 MISSÃO, VISÃO, VALORES INSTITUCIONAIS E DIRETRIZES DO PLANEJAMENTO ESTRATÉGICO

A MISSÃO representa a razão de ser da organização ou o motivo pelo qual ela existe. Por isso mesmo, é uma declaração que orienta todas as suas ações e decisões. A missão deve comunicar de forma clara e objetiva a todos na organização o que se espera de seu trabalho

e também como ela deseja ser reconhecida por seus clientes. Responde à questão: “por que ou para que existimos?”. Eis a **MISSÃO** do ITI:

ATUAR NA INOVAÇÃO, REGULAÇÃO E PROVIMENTO DE SOLUÇÕES TECNOLÓGICAS QUE GARANTAM SEGURANÇA E CONFIANÇA DIGITAL A DOCUMENTOS E TRANSAÇÕES ELETRÔNICAS.

VISÃO é como a organização deseja ser reconhecida. É o sonho a ser nutrido pelos dirigentes, gestores, servidores e todas as partes interessadas. Ela deve refletir o avanço da organização no desempenho de sua finalidade e estabelecer o posicionamento futuro a ser almejado por todos, em busca dos resultados projetados no planejamento estratégico. A visão de futuro deve estar atenta aos sinais de mudança, para identificar as oportunidades e ameaças, orientando os esforços para inspirar e transformar um propósito em ação.

Eis a **VISÃO** do ITI:

SER REFERÊNCIA NACIONAL E INTERNACIONAL EM TECNOLOGIAS PARA SEGURANÇA E CONFIANÇA DIGITAL.

VALORES INSTITUCIONAIS - os valores institucionais representam os princípios que devem nortear as ações e a conduta dos servidores, gerentes e dirigentes da organização. Eles formam o código de conduta e são inegociáveis. Compõem os princípios éticos e o estofo moral que deverão ser respeitados enquanto a organização busca cumprir sua missão e atingir os objetivos de sua visão. Eles orientam e impõem limites à tomada de decisões e determinam a forma como a organização se comporta e interage com suas partes interessadas.

Ética: padrões de conduta materializados na verdade dos fatos, honestidade, moralidade, coerência e probidade administrativa.

Transparência: disponibilização de dados e informações que permitam a avaliação das contribuições e impactos econômicos, sociais e ambientais das atividades, ressalvadas as informações confidenciais.

Integridade: combate a todo e qualquer mecanismo de corrupção, desvio de finalidade, desperdício de recursos públicos, contratações irregulares e sobreposição de interesse privado ao público.

Responsabilidade Social: responsabilidade pelos resultados e impactos das ações no meio natural e social afetados, com esforços no sentido de cumprir as obrigações para o bem-estar da coletividade.

Segurança: soluções com garantia de segurança, integridade, autenticidade e confidencialidade em transações e documentos eletrônicos.

Validade Jurídica: soluções adequadas às normas legais e regulamentares a fim de que transações e documentos eletrônicos tenham validade jurídica.

Inovação: soluções inovadoras que garantam confiança e segurança em transações e documentos eletrônicos.

O Planejamento Estratégico do Instituto Nacional de Tecnologia da Informação – ITI, elaborado para o período de 2019-2022, utilizada como ferramenta de proposição e monitoramento o *Balanced Scorecard – BSC*. Trata-se de um sistema de gestão e medição de desempenho derivado das estratégias e capacidades da organização. Tem como principal objetivo o alinhamento de toda a organização com suas estratégias, por meio da tradução da missão e da visão da organização em um conjunto de objetivos, indicadores de desempenho e projetos estratégicos estruturados.

Publicado: Quarta, 23 de Janeiro de 2019, 10h28 | Última atualização em Quarta, 23 de Janeiro de 2019, 10h28 (www.iti.gov.br)

O Instituto Nacional de Tecnologia da Informação – ITI publicou na última segunda-feira, 21, o **Planejamento Estratégico do Instituto para o período de 2019 a 2022**. No documento são detalhadas as ações que serão adotadas pelo ITI, no período determinado, com intuito de promover o melhor uso dos recursos disponíveis para atendimento das demandas da sociedade.

O documento destaca que o foco principal do Instituto, nos próximos quatro anos, será a ampliação do uso da certificação digital no padrão da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil e das novas tecnologias associadas à identificação e assinatura digital para melhor atender ao cidadão. Para isso, serão adotadas medidas como: promoção de soluções tecnológicas para a prestação de serviços digitais confiáveis, disseminação do uso das tecnologias de assinatura digital para os documentos eletrônicos e fomento de acordos

internacionais para interoperabilidade de Infraestruturas de Chaves Públicas e reconhecimento mútuo de assinaturas digitais.

O Planejamento apresenta, de forma detalhada, os indicadores estratégicos para cada objetivo listado, os projetos que serão colocados em prática e a criticidade de cada ação. Para acompanhamento das ações propostas, o documento institui o Comitê de Governança e Planejamento Estratégico – CGPE, que será responsável por certificar que os objetivos estratégicos estão sendo atingidos mediante a correta gestão da transformação, entrega dos resultados pactuados e monitoramento tempestivo da rotina.

DIRETRIZES DO PLANEJAMENTO ESTRATÉGICO:

As diretrizes do Planejamento Estratégico revelam-se nos direcionadores estratégicos do PE-ITI 2019-2022 que são os seguintes:

I. Prover soluções tecnológicas para a prestação de serviços digitais confiáveis;
II. Massificar a certificação digital padrão ICP Brasil e novas tecnologias associadas à identificação e assinatura digital;
III. Disseminar e fomentar o uso das tecnologias de assinatura digital para os documentos eletrônicos;
IV. Fomentar acordos internacionais para interoperabilidade de Infraestruturas de Chaves Públicas e reconhecimento mútuo de assinaturas digitais e
V. Tornar-se autossustentável financeiramente, mediante modelo de arrecadação que desonere o orçamento público.

1.5 PRINCIPAIS INSTRUMENTOS LEGAIS INTERNOS RELATIVOS À ÁREA DE INTEGRIDADE

O decreto nº 9.203, de 22 de novembro de 2017, dispõe sobre a política de governança da administração pública federal direta, autárquica e fundacional e avança na concretização da referida política ao determinar em seu art. 20 que o Ministério da Transparência e Controladoria-Geral da União, no prazo de cento e oitenta dias, contado da data de entrada em vigor do já referido Decreto, estabelecerá os procedimentos necessários à estruturação,

à execução e ao monitoramento dos programas de integridade dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

Estabelece, também, em seu art.2º, inciso I, a definição de **governança pública** como um conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade e tem a **INTEGRIDADE** como um dos seus princípios (art. 3º, inciso II).

Alinhado com essa política, o ITI vem instituindo instrumentos legais internos que cooperam na ratificação da INTEGRIDADE como cultura do Órgão. Ei-los:

REGIMENTO INTERNO DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI – aprovado pela Portaria n. 20, de 28 de fevereiro de 2018.

PLANEJAMENTO ESTRATÉGICO DO ITI 2019 – 2022 (publicado no site do ITI – www.iti.gov.br).

PROGRAMA DE INTEGRIDADE E COMPLIANCE (orientações para o ITI)

CÓDIGO DE ÉTICA – (EM ELABORAÇÃO).

PLANO DE INTEGRIDADE E COMPLIANCE DO ITI (EM ELABORAÇÃO).

PORTARIA n. 01, de 21 de janeiro de 2019 - institui a unidade responsável pela gestão de Integridade *e Compliance* no âmbito do Instituto Nacional de Tecnologia da Informação.

PORTARIA Nº 79, de 31 de dezembro de 2018 - dispõe sobre a Política de Segurança da Informação e Comunicações do Instituto Nacional de Tecnologia da Informação.

PORTARIA Nº 62, de 04 de outubro de 2018 do ITI - institui Comitê de Governança do Planejamento Estratégico 2019-2022 do Instituto Nacional de Tecnologia da Informação – ITI, e dá outras providências.

PORTARIA N. 33, de 20 de junho de 2017 – institui o Comitê de Governança, Riscos, Controles e Governança Digital – CGRC-GD

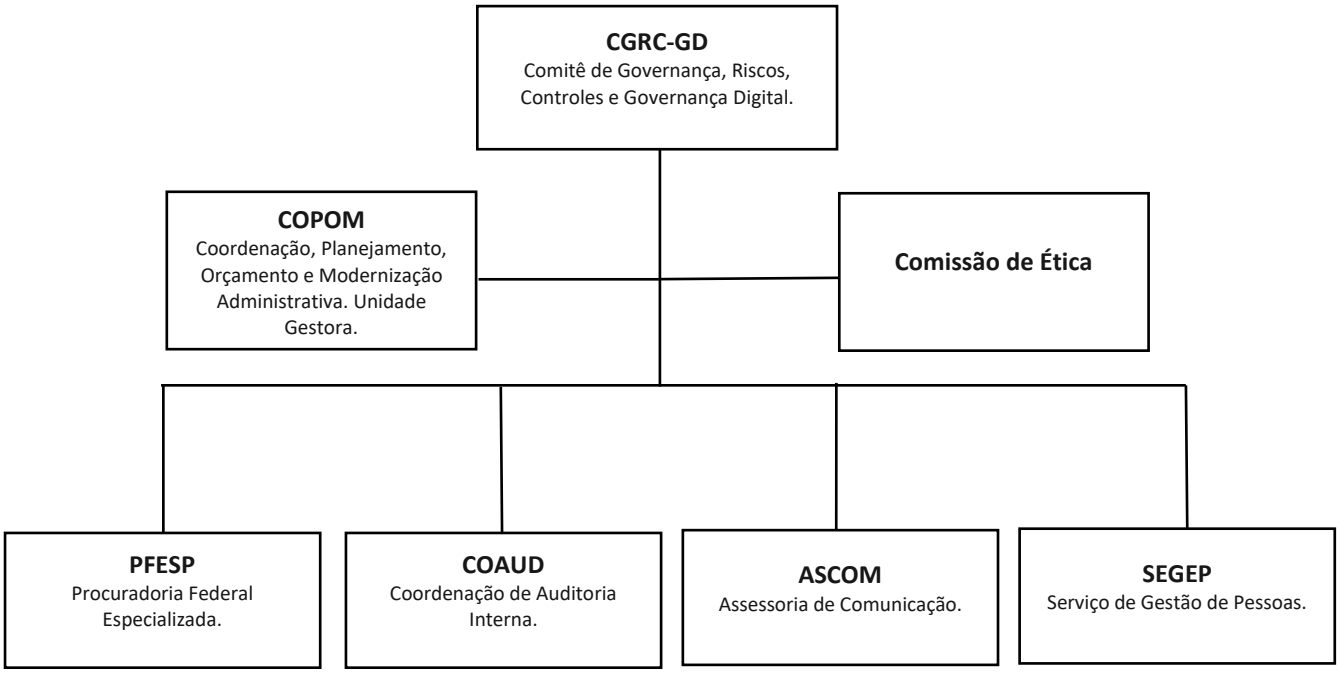
PORTARIA Nº 40, de 28 de junho de 2018 - institui a Política de Gestão de Riscos do Instituto Nacional de Tecnologia da Informação – ITI.

PORTARIA nº 16 , de 9 de fevereiro de 2018. Dispõe sobre a Política de Governança de Tecnologia da Informação e Comunicação do Instituto Nacional de Tecnologia da Informação.

PLANILHA DE LEVANTAMENTO DA SITUAÇÃO DAS UNIDADES DO ITI E RESPECTIVOS INSTRUMENTOS QUE ATUAM DIRETAMENTE NA MANUTENÇÃO DA CULTURA DE INTEGRIDADE E COMPLIANCE DO ÓRGÃO.

FUNÇÃO DE INTEGRIDADE E COMPLIANCE	UNIDADE/INSTRUMENTO DE INTEGRIDADE	A UNIDADE E INSTRUMENTO EXISTEM?	ÁREA RESPONSÁVEL PELA CRIAÇÃO DA UNIDADE/INSTRUMENTO	
			RESPONSÁVEL	PRAZO
Promoção da ética e regras de conduta para servidores.	Comissão de Ética/Código de Ética e Conduta.	NÃO	COAUD	60 DIAS
Cumprimento das normas e legislações vigentes.	Procuradoria Federal Especializada/Portaria Nº33 de 2017. Prestar assessoria júridica as áreas em relação às normas e legislações vigentes.	SIM		
Estruturação, execução e acompanhamento do Programa de Integridade e Compliance em conformidade com Planejamento Estratégico do ITI.	COPOM - Coordenação de Planejamento, Orçamento e Modernização Institucional/Portaria Nº33 de 2017. Designada como Unidade Gestora da Integridade e Compliance.	SIM		
Realizar capacitação do servidor direcionada ao Programa de Integridde e Compliance.	CEGEP - Serviço de Gestão de Pessoas/Portaria Nº33 de 2017. Promover a ética e regras de conduta para servidores.	SIM		
Transparência ativa e acesso a informação.	ASCOM- Assessoria de Comunicação/Portaria Nº 33 de 2017. Comunicar e desseminar as ações do Programa de Integridade e Compliance e promover a transparência ativa e do acesso a informação.	SIM		
	Adoção do Sistema e-SIC.	NÃO	SEGEP	180 DIAS
Tratamento de conflitos de interesses e nepotismo.	COAUD - Coordenação ou Assessoria de Auditoria Interna/Portaria Nº 33 de 2017. Observar a Lei 12.813 de 2013; Decreto Nº7 .203 de 2010 e Portaria Interministerial Nº 33 (MPDG/MT e CGU), 2013.	SIM		
Funcionamento de canais de denúncias.	CEGEP - Serviço de Gestão de Pessoas/Portaria Nº33 de 2017. Promover a ética e regras de conduta para servidores.	SIM		
	Adoção e-OUV.	SEGEP		
Funcionamento de controles internos e cumprimento de recomendações da auditoria.	COAUD - Coordenação de Auditoria Interna/RI. Mantém contínuo intercâmbio com os órgãos de Controle; monitora a execução a Política de Gestão de Riscos e Governaça Digital, implementadas no ITI; analisa e fiscaliza os atos e fatos administrativos em seus aspectos econômicos, financeiros, orçamentários, patrimoniais e legais e analisa a eficiência e eficácia dos controles internos, buscando o seu constante aprimoramento. Apurar, investigar e emitir parecer acerca do descumprimento do Programa de Integridade e Compliance/Portaria Nº 33 de 2017.	SIM		
Procedimentos de responsabilização.	COAUD - Coordenação ou Assessoria de Auditoria Interna/Portaria Nº33 de 2017. Implementar procedimentos de responsabilização em conjunto com as demais unidades, observando o Decreto Nº 5.480 de 2005 e Portarias da CGU Números: 335/2006, 1.043/2007 e 1.196/2017.	SIM		

1.6 ESTRUTURAS DE GESTÃO DA INTEGRIDADE



A presente estrutura foi criada pela Portaria n. 33 de 20 de junho de 2017 do ITI e aqui torna-se oportuno ratificar algumas das recomendações contidas no Programa de Integridade e *Compliance* imprescindíveis ao seu êxito e maturidade, já que a inobservância delas pode comprometer também o sucesso da implantação, funcionamento e êxito do Plano de Integridade e *Compliance* do Órgão. Quais sejam:

a) É condição essencial se criar a Comissão de Ética e respectivo Código de Ética. O Código de Ética de um Instituto pode ser comparado à Constituição de um país. É nele que constarão as regras básicas e valores nos quais os integrantes do Órgão devem pautar suas respectivas condutas;

b) Comunicação e Treinamentos - deve-se definir as áreas e pessoas que precisam de treinamentos, de acordo com os riscos de Integridade e *Compliance* específicos de cada área da Autarquia. Ademais, deve-se adotar mecanismos de mensuração da efetividade dos treinamentos e adequação destes aos diferentes públicos;

c) Fazer análise periódica de riscos e monitoramento constante;

d) Ter um processo bem definido de recebimento, tratamento e apuração das denúncias e

e) Ter profundo comprometimento com a incorporação e manutenção da cultura de Integridade e *Compliance* nas suas atividades e negócios, inclusive com o empenho de tempo, recursos humanos e financeiros.

2. UNIDADE RESPONSÁVEL PELO PLANO DE INTEGRIDADE

A Portaria n. 01, de 21 de janeiro de 2019 instituiu unidade responsável pela gestão da Integridade e Compliance no âmbito do Instituto Nacional de Tecnologia da Informação.

A Coordenação de Planejamento, Orçamento e Modernização Institucional – COPOM foi designada pela referida portaria para coordenar a estruturação, execução e monitoramento do Programa de Integridade e Compliance no âmbito do ITI.

Competência da COPOM:

I – coordenar a elaboração e revisão do Plano de Integridade e Compliance, com vistas à prevenção e à mitigação de vulnerabilidades eventualmente identificadas;

II – coordenar a implementação do Programa de Integridade e Compliance e exercer o seu monitoramento contínuo, visando seu aperfeiçoamento na prevenção, detecção e combate à ocorrência de atos lesivos;

III – atuar na orientação e treinamento dos servidores do ITI com relação aos temas atinentes ao Programa de Integridade e Compliance e

IV – promover outras ações relacionadas à gestão da Integridade e Compliance em conjunto com as demais áreas do ITI.

Atribuições da COPOM:

I - submeter à aprovação do Diretor-Presidente do ITI a proposta de Plano de Integridade e Compliance e revisá-lo periodicamente;

II – levantar a situação das unidades relacionadas ao Programa de Integridade e Compliance e, caso necessário, propor ações para sua estruturação ou fortalecimento;

III – apoiar a Unidade de Gestão de Riscos no levantamento de riscos para a Integridade e Compliance e proposição de plano de tratamento;

IV – coordenar a disseminação de informações sobre o Programa de Integridade e Compliance no ITI;

V – planejar e participar de ações de treinamento relacionados ao Programa de Integridade e Compliance no ITI;

VI – identificar eventuais vulnerabilidades à Integridade e Compliance nos trabalhos desenvolvidos pelo ITI, propondo, em conjunto com outras unidades, medidas para mitigação;

VII – monitorar o Programa de Integridade e Compliance do ITI e propor ações para o seu aperfeiçoamento e

VIII – propor estratégias para expansão do programa para fornecedores e terceiros que se relacionem com o ITI.

A referida Portaria também preceitua que todos os agentes públicos, gestores, dirigentes, e unidades organizacionais do Órgão devem prestar, no âmbito de suas respectivas competências e atribuições, apoio aos trabalhos desenvolvidos pela COPOM, Unidade de Gestão da Integridade e Compliance.

Preceitua, ainda, que o Diretor-Presidente proverá o apoio técnico e administrativo para o pleno funcionamento da Coordenação de Planejamento, Orçamento e Modernização Institucional – COPOM, como Unidade de Integridade e Compliance.

3. RISCOS PRIORITÁRIOS À INTEGRIDADE

Riscos à Integridade são eventos relacionados à corrupção, fraudes, irregularidades e\ou desvios éticos e de conduta, que possa comprometer os valores e padrões preconizados pelo ITI e a realização de seus objetivos.

No entender de Wagner Giovanini, no livro intitulado *COMPLIANCE*, "a excelência na prática", uma reflexão abrangente torna-se valiosa para se identificarem os riscos, quais sejam:

- Quais são as legislações aplicáveis no meu ramo de atuação? Aqui se valorizam todos os aspectos legais.
- Quais são as relações externas e internas a que minha organização está sujeita?
- Que processos da minha organização possibilitam algum risco para o meu negócio?
- Que atividades do meu dia a dia favorecem algum risco para a imagem do Órgão e/ou para os funcionários? Pode-se elencar a cessão ou recebimento de brindes, oferecimento de almoços a terceiros, doações, patrocínios etc.

- Quais são os atores do meu Órgão? Acontece muita rotatividade de pessoal? Existem pessoas novas na organização? Há maturidade suficiente nos cargos-chaves e os líderes estão preparados? As nossas pessoas estão devidamente qualificadas? Agem de maneira íntegra e estão alinhadas com os princípios do Órgão?
- Há um entendimento claro dos princípios e valores de nosso Instituto?

Inicialmente, far-se-á o levantamento prévio dos principais riscos do ITI por meio de FORMULÁRIO DE REGISTRO DE RISCOS (ANEXO I), que será distribuído por e-mail para os respectivos responsáveis por cada unidade do Órgão. Será encaminhado, também, um formulário de registro de riscos exemplificativo para auxiliar no preenchimento do já citado formulário (ANEXO II). O objetivo deste procedimento é fazer a detecção fidedigna dos possíveis riscos de Integridade e Compliance, se já houve manifestação deles na unidade e quais fatores motivaram sua ocorrência.

Assim, para o levantamento dos riscos de integridade de cada unidade, o responsável deve fazer a seguinte pergunta: que atividades do meu dia a dia podem ser suscetíveis a algum risco de integridade?

Vale explicitar que os Fatores de Risco dizem respeito a eventos que podem propiciar a manifestação do risco, como por exemplo, a inobservância de normas, ausência de treinamento, comportamento antiético, etc.

Os formulários devem ser devolvidos no prazo de 30 (trinta) dias, a partir da data de recebimento, para a Unidade Gestora da Integridade e Compliance, ou seja, a COPOM.

De posse de todos os formulários preenchidos, a COPOM desenvolverá um Plano de Ação com a alta administração, com base no grau de impacto X probabilidade na Instituição de cada risco. Destarte, para que não haja desperdício de esforços, os riscos a serem inicialmente gerenciados pelo Plano de Integridade e Compliance precisam ser os mais relevantes para o Instituto, isto é, os de maior impacto e probabilidade dentro de um limite previamente definido pela alta administração. Para tanto, para cada risco registrado deve ser identificada a possibilidade de sua ocorrência (probabilidade) e a gravidade das consequências para a instituição, caso se concretize (impacto).

O processo de avaliação global de um conjunto de riscos será efetivado pela ferramenta denominada MAPA DE CALOR, que apresenta de forma simples e visual suas relevâncias

através do cruzamento das probabilidades e dos níveis de impacto em um gráfico. Ele pode designar as seguintes pontuações para a probabilidade e impacto do risco:

- **Muito baixa (1)** – baixíssima possibilidade de o evento ocorrer;
- **Baixa (2)** – o evento ocorre raramente;
- **Média (3)** – o evento já ocorreu algumas vezes e pode voltar a ocorrer e
- **Alta (4) –** o evento já ocorreu repetidas vezes e provalvemente voltará a ocorrer outras tantas.

Após desenvolver o Mapa de Calor, a COPOM, sob orientação da alta direção, estabelecerá a ordem de prioridade para o tratamento dos riscos, quais sejam:

- **Aceitar** – o Instituto decide não fazer nada em relação ao risco. A sua probabilidade e impacto são tão baixos que não justificam a criação de controles para mitigação; ou os controles existentes já resguardam boa parte de suas consequências;
- **Transferir** – o risco possui probabilidade e impacto tão altos que o Instituto não pode suportar e decide transferi-los a outra entidade.
- **Mitigar** – o Instituto decide atuar para reduzir a probabilidade e/ou impacto do risco, tornando-o menor ou eliminando.
- **Evitar** – envolve alterar o plano de gerenciamento do projeto para eliminar a ameaça, eliminando a causa do problema.

O Mapa de Calor está bem detalhado e exemplificado no Programa de Integridade e Compliance.

4. MONITORAMENTO E ATUALIZAÇÃO PERIÓDICA

O monitoramento é o acompanhamento contínuo das ações previstas neste Plano de Integridade e aprovadas pela Alta Administração, com vistas a avaliar os resultados alcançados pelo Programa.

No escopo do monitoramento contínuo, incluem-se as medidas de tratamento dos riscos à integridade, as iniciativas de capacitação de líderes e colaboradores, as medidas de fortalecimento das instâncias relacionadas ao tema e os meios de comunicação e reporte utilizados pelo Programa.

O Plano de Ação (ANEXO III) que traduz a efetivação do monitoramento será gerido pela COPOM e o seu preenchimento está exemplificado no ANEXO IV.

Além do Plano de Ação, outras Medidas e Ações de Integridade são imprescindíveis para o sucesso do Plano de Integridade e *Compliance*, apresentadas no Programa de Integridade e *Compliance* como BOAS PRÁTICAS. Quais sejam:

- CRIAR CÓDIGO DE ÉTICA que apresente de forma clara e precisa os valores e condutas esperados e comportamentos a serem evitados para todos os servidores do ITI, incluindo membros da alta direção, funcionários terceirizados e estagiários.
    1. Instituir Comissão de Ética com estrutura e recursos adequados.

O Decreto n. 1.171/1994 estabelece que em todos os órgãos e entidades da Administração Pública Federal, indireta, autárquica e fundacional, ou em qualquer órgão ou entidade que exerça atribuições delegadas pelo poder público, deverá ser criada uma Comissão de Ética, encarregada de orientar e aconselhar sobre a ética profissional do servidor no tratamento com as pessoas e com o patrimônio público.

- POLÍTICAS DE COMUNICAÇÃO E TREINAMENTO – comunicar as regras do Código de Ética em linguagem acessível transmitindo sua mensagem independentemente do nível de escolaridade do público alvo.
    1. Divulgar entre todos os servidores da Autarquia os membros e contatos da Comissão de Ética e os casos em que essa instância pode ser acionada.
    2. Promover eventos periódicos para treinamentos e discussões de questões éticas, atentando-se para o público-alvo de maior risco envolvendo inclusive a alta direção.
- DISPONIBILIZAR CANAIS DE FÁCIL ACESSO PARA REALIZAÇÃO DA DENÚNCIA.
    1. Estabelecer regras claras para a proteção dos denunciantes, inclusive permitindo a realização de denúncias anônimas.
    2. Estabelecer fluxo claro de encaminhamento das denúncias e posterior apuração.
    3. Monitorar e avaliar as possíveis exposições do Instituto a riscos e comunica-los à alta direção.

- MEDIDAS DE CONTROLE E DISCIPLINARES
    1. Os problemas detectados, especialmente os que apresentem indícios de gravidade, devem ser investigados com celeridade. A atuação correicional tem efeito desmotivador para cometimento de novas irregularidades dentro da organização
    2. Garantir estrutura e independência da unidade responsável pela gestão dos controles internos.
    3. Promover reportes periódicos e tempestivos à alta direção e aos órgãos centrais de controle interno e externo acerca de medidas de controle e disciplinares em curso.
    4. Conduzir e documentar as investigações de violação das normas de integridade com base em procedimentos de investigação formalmente definidos pelo Instituto.
- AÇÕES E REMEDIAÇÃO
    1. Compilar regularmente os casos de quebra de integridade buscando analisar as principais tendências e causas das recomendações de auditoria e sanções aplicadas, de modo a promover eventuais alterações em políticas, procedimentos ou controles.
    2. Capacitar os membros de comissão de processos disciplinares a identificar e sugerir em seus relatórios.

5. ANEXOS

ANEXO I

FORMULÁRIO DE REGISTRO DE RISCO			
ÁREA:			
PROCESSO:			
RISCO:			
DESCRIÇÃO DO RISCO:			
#	FATORES DE RISCO	CONTROLES EXISTENTES	ANÁLISE
I			
II			
III			

ANEXO II (EXEMPLO DO ANEXO I)

FORMULÁRIO DE REGISTRO DE RISCO PREENCHIDO PARA EXEMPLIFICAÇÃO			
ÁREA: GESTÃO DE PESSOAS			
PROCESSO: NOMEAÇÃO OU DESIGNAÇÃO DE PESSOA PARA CARGO DE EM COMISSÃO			
RISCO: NEPOTISMO			
DESCRIÇÃO DO RISCO: DESIGNAÇÃO OU DESIGNAÇÃO DE FAMÍLIAR DE MINISTRO DE ESTADO, FAMILIAR DA MÁXIMA AUTORIDADE ADMINISTRATIVA CORRESPONDENTE OU FAMILIAR DE OCUPANTE DE CARGO EM COMISSÃO OU FUNÇÃO DE CONFINÇA PARA CARDO EM COMISSÃO OU FUNÇÃO DE CONFIANÇA.			
#	FATORES DE RISCO	CONTROLES EXISTENTES	ANÁLISE
I	DESCONHECIMENTO DO DECRETO Nº 7.203/2010.	SERVIDORES DA COORDENAÇÃO-GERAL DE RECURSOS HUMANOS RECEBERAM UMA CAPACITAÇÃO NA ÉPOCA DA AROVAÇÃO DO DECRETO. NÃO HOUVE CAPACITAÇÕES POSTERIORES APESAR DE VÁRIOS SERVIDORES TEREM SAÍDO E CHEGADO À ÁREA.	APESAR DE EXISTIR PREVISÃO DE CAPACITAÇÃO, ELA NÃO FOI CONTINUADA.
II	AUSÊNCIA DE PROCEDIMENTO DE VERIFICAÇÃO DE LAÇOS DE PARENTESCO DAS PESSOAS NOMEADAS, CONTRATADS OU DESIGNADAS COM O MINISTRO DE ESTADO, AUTORIDADE MÁXIMA CORRESPONDENTE OU OCUPANTES DE CARGOS EM COMISSÃO E FUNÇÕES DE CONFIANÇA.	NENHUMA.	NÃO HÁ MEDIDAS.
III	AUSÊNCIA DE REGRAS CLARAS PARA OCUPAÇÃO DE CARGOS EM COMISSÃO E FUNÇÕES DE CONFIANÇA.	NORMATIVO RECENTE ESTIPULOU REGRAS CLARAS PARA OCUPAÇÃO DE CARGOS DAS SOMENTE ATÉ NÍVEL 3 E EM ALGUMAS UNIDADE DO ÓRGÃO.	MEDIDS NÃO ABARCAM TODOS OS CARGOS.

ANEXO III

PLANO DE AÇÃO					
FATOR DE RISCO	RISCO ASSOCIADO	RELEVANCIA PROBABILIDADE X IMPACTO	MEDIDAS DE INTEGRIDADE EXISTENTES	RECOMENDAÇÃO	DETALHAMENTO

ANEXO IV (EXEMPLO DO ANEXO III)

PLANO DE AÇÃO PARA EXEMPLIFICAÇÃO					
FATOR DE RISCO	RISCO ASSOCIADO	RELEVANCIA PROBABILIDADE X IMPACTO	MEDIDAS DE INTEGRIDADE EXISTENTES	RECOMENDAÇÃO	DETALHAMENTO
MEMBROS DA COMISSÃO DE LICITAÇÃO NÃO SÃO ORIENTADOS EM COMO RECEBER REPRESENTANTES DE EMPRESAS.	FRAUDE À LICITAÇÃO.	PROBABILIDADE(2)X IMPACTO(4)=RELEVÂNCIA(8)	NENHUMA.	PUBLICAR ORIENTAÇÃO INTERNA QUANTO AO RECEBIMENTO DE REPRESENTANTES. CAPACITAR E ORIENTAR OS MEMBROS DA COMISSÃO DE LICITAÇÃO.	RESPONSÁVEL: GESTOR DA ÁREA/COORDENAÇÃO DE CAPACITAÇÃO. PRAZO: 6 MESES MONITORAMENTO: ORIENTAÇÃO PUBLICADA/CAPACITAÇÃO REALIZADA/QUESTIONÁRIOS COM SERVIDORES POLÍTICA.
POLÍTICA DE PREVENÇÃO DE CONFLITO DE INTERESSES NÃO FOI TOTALMENTE INSTITUIDA PELO ÓRGÃO.	CONFLITO DE INTERESSES.	PROBABILIDADE(1)X IMPACTO(2)=RELEVÂNCIA(2)	CAMPANHA DE SENSIBILIZAÇÃO REALIZADA NA INTRANET. CADASTRO DO ÓRGÃO O SeCI.	IMPLEMENTAR MEDIDAS VOLTADAS À ALTA DIREÇÃO. DIVULGAÇÃO DO SeCI ENTRE OS SERVIDORES.	RESPONSÁVEL: GESTOR DA ÁREA/COORDENAÇÃO DE AUDITORIA INTERNA. PRAZO: 4 MESES MONITORAMENTO: MEDIDAS DE SENSIBILIZAÇÃO DESENVOLVIDAS/APLICADAS E DIVULGAÇÃO DO SeCI REALIZADA.
PROCESSO DE CONCESSÃO DE LICENÇAS NO ÓRGÃO NÃO É TOTALMENTE TRANSPARENTE.	PRESSÕES EXTERNAS INDEVIDAS/ABUSO DE PODER.	PROBABILIDADE(2)X IMPACTO(3)=RELEVÂNCIA(6)	PUBLICAÇÃO DOS RESULTADOS NO DIÁRIO OFICIAL.	GARANTIR TRANPARÊNCIA EM TODO PROCESSO DE CONCESSÃO DE LICENÇAS, DA FASE INTERNA À PUBLICAÇÃO DOS RESULTADOS, ATRAVÉS DE MEDIDAS DE TRANSPARÊNCIA ATIVA.	RESPONÁVEL: SECRETARIA EXECUTIVA/GESTOR DA ÁREA. PRAZO: 12 MESES. MONITORAMENTO: MEDIDAS DE TRANSPARÊNCIA ADOTADAS.
SERVIDORES RESPONSÁVEIS PELA IMPOSIÇÃO DE MULTAS ADMINISTRATIVAS CONCENTRAM MUITO PODER DISCRICIONÁRIO.	SUBORNO/ABUSO DE PODER	PROBABILIDADE(3)X IMPACTO(4)=RELEVÂNCIA(12)	SERVIDORES ESTÃO SUJEITOS A AUDITORIAS ANUAIS PELOS ÓRGÃOS DE CONTROLE.	DESCONCENTRAR PODER DECISÓRIO ATRAVÉS DE REFORMULAÇÃO DE COMPETÊNCIAS. INSTITUIR INSTÂNCIA DE SUPERVISÃO. VERIFICAR EVOLUÇÃO PATRIMONIAL DOS SERVIDORES DA ÁREA.	RESPONÁVEL: SECRETARIA EXECUTIVA/AUDITORIA INTERNA/CORREGEDORIA./GESTOR DA ÁREA. PRAZO: 12 MESES. MONITORAMENTO: MEDIDAS DE TRANSPARÊNCIA ADOTADAS.