

**Relatório Anual de Avaliação da Gestão do Instituto
Nacional de Tecnologia da Informação – ITI**

2017

Brasília – 2018

Presidência da República
Secretaria-Geral
Secretaria de Controle Interno
Coordenação-Geral de Auditoria de Gestão

RELATÓRIO DE AUDITORIA ANUAL DE CONTAS
Órgão: Instituto Nacional de Tecnologia da Informação – ITI

SUMÁRIO

I.	INTRODUÇÃO	4
II.	AVALIAÇÃO DA GESTÃO	5
A.	GESTÃO FINALÍSTICA	5
A.I.	GOVERNANÇA E GESTÃO DE TECNOLOGIA DA INFORMAÇÃO	5
A.II.	GERENCIAMENTO DE RISCOS	7
B.	MECANISMOS DE GOVERNANÇA E INTEGRIDADE	7
C.	CONCLUSÃO	8
D.	RECOMENDAÇÕES	9
III.	ACHADOS DE AUDITORIA	13
1.	GOVERNANÇA E GESTÃO EM TECNOLOGIA DA INFORMAÇÃO	19
1.1.	MECANISMOS DE GOVERNANÇA INSTITUCIONAL	20
1.2.	GOVERNANÇA DE TI	21
1.2.1.	ESTRATÉGIAS E PLANOS INSTITUCIONAIS DE TI	22
1.3.	MECANISMOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	23
1.4.	AQUISIÇÕES DE SOLUÇÕES DE TI	24
2.	GERENCIAMENTO DE RISCOS	27
2.1.	ALTERAÇÃO DO ÓRGÃO SUPERVISOR DO ITI	27
2.2.	ADOÇÃO DE TECNOLOGIA COM FALHAS	28
2.3.	MUDANÇA INTEMPESTIVA NOS REQUISITOS QUE AFETAM A INFRAESTRUTURA	29
3.	PROCESSO DE COMPRAS E CONTRATAÇÕES	29
3.1.	PREGÕES	30
4.	AVALIAÇÃO DOS MECANISMOS DE TRANSPARÊNCIA E CONTROLE SOCIAL - OUVIDORIA	31
4.1.	CONTROLE SOCIAL – OUVIDORIA	31
4.2.	AVALIAÇÃO DOS MECANISMOS DE TRANSPARÊNCIA E CONTROLE SOCIAL	33
5.	AVALIAÇÃO DA GESTÃO DE PESSOAS	36
5.1.	ASPECTOS QUANTITATIVOS E QUALITATIVOS	40

I. INTRODUÇÃO

1. Trata-se de relatório de auditoria de gestão, que contempla os resultados da auditoria realizada sobre o processo anual de contas 2017 do Instituto Nacional de Tecnologia da Informação – ITI, elaborado de forma a compor o processo de trabalho do controle externo destinado a avaliar e julgar o desempenho e a conformidade da gestão dos agentes abrangidos pelos incisos I, III, IV, V e VI do art. 5º da Lei nº 8.443/92, com base em documentos, informações e demonstrativos de natureza contábil, financeira, orçamentária, operacional ou patrimonial.

2. A presente auditoria teve por objetivo fomentar a boa governança pública, aumentar a transparência, promover melhorias na prestação de contas da Unidade, induzir a gestão pública para resultados e fornecer opinião sobre as contas a serem julgadas pelo Tribunal de Contas da União.

3. Em atendimento à determinação contida na Ordem de Serviço nº 2018/026 e às diretrizes emanadas da Decisão Normativa TCU nº 163, de 6 de dezembro de 2017, bem como em observância aos itens definidos na ata da reunião, de 7 de dezembro de 2017, realizada entre a Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (Sefti/TCU) e a Secretaria de Controle Interno da Secretaria-Geral da Presidência da República (CISSET/SG/PR), apresenta-se neste documento a consolidação das análises realizadas segundo os critérios definidos em instrumento de planejamento dos trabalhos.

4. O escopo definido abrange: mapeamento dos principais processos e mecanismos de governança instituídos para operacionalizar e fiscalizar a ICP-Brasil; avaliação dos mecanismos de gerenciamento de riscos instituídos e em funcionamento; avaliação da gestão de pessoas com foco em aspectos quantitativos e qualitativos; avaliação dos mecanismos de transparência e controle social; e visão gerencial dos processos de compras e contratações da UPC.

5. A abordagem adotada pela Secretaria de Controle Interno, para atender ao escopo definido com o TCU e avaliar a gestão da UPC no exercício de 2017, foi tratada sob dois aspectos: avaliação da gestão finalística e avaliação dos mecanismos de governança.

6. Em razão do entendimento acima exposto, os trabalhos de campo foram realizados na sede do ITI, em Brasília, no período de 20 a 31 de agosto de 2018, por meio de exames e consolidação de informações coletadas referentes ao exercício de 2017 e a partir da análise da prestação de contas apresentada pela Unidade Auditada.

7. A versão preliminar do Relatório de Auditoria de Gestão foi disponibilizada no dia 4/9/2018 para que a Sead pudesse apresentar as suas manifestações ao relatório até o dia 10/9/2018. Ressaltamos que todas as manifestações da unidade foram analisadas e que destacamos aqui no relatório aquelas que possuem o condão de alterar algum entendimento da Equipe de

Auditoria. Por outro lado, as manifestações meramente explicativas não serão abordadas e compõem o acerto de papéis de trabalho da auditoria.

8. Convém anotar que esse Relatório de Auditoria encontra-se dividido da seguinte forma: Avaliação da Gestão, que contém a síntese das análises realizadas e conclusões obtidas sobre os itens do escopo; e Achados de Auditoria, seção em que são apresentados os Exames de Auditoria.

9. Nesse sentido, em observância às normas de auditoria aplicáveis ao Serviço Público Federal, apresentam-se a seguir os resultados dos exames realizados.

II. AVALIAÇÃO DA GESTÃO

A. GESTÃO FINALÍSTICA

10. No que se refere à atuação finalística do órgão, os trabalhos tiveram por objetivo avaliar os controles internos relativos à governança e gestão em Tecnologia da Informação e o gerenciamento de risco instituído pelo Instituto Nacional de Tecnologia da Informação – ITI.

11. No que diz respeito à análise da governança e gestão de tecnologia buscou-se realizar uma avaliação da conformidade da gestão do ITI em relação aos normativos que regem a tecnologia da informação de órgãos/entidades do setor público bem como a aderência a boas práticas já sedimentadas no mercado e que são mundialmente aceitas nessa área de negócio.

12. Por outro lado, no que tange o gerenciamento de risco, buscou-se elencar os principais riscos ao qual o negócio do TI está submetido e as possíveis ações realizadas pelo ITI para mitigá-los.

13. Ante o exposto, em observância às normas de auditoria aplicáveis ao Serviço Público Federal, apresenta-se a seguir a avaliação da UPC quanto à gestão finalística das supracitadas áreas em face da consecução dos objetivos estabelecidos em relação às competências do ITI em relação à ICP-Brasil, tais como: coordenação, fiscalização, auditoria, normatização, homologação, guarda da estrutura física, etc.

A.I. GOVERNANÇA E GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

14. Com relação à governança e gestão de tecnologia da Informação podemos destacar o papel atuante dos comitês formalmente instituídos pela UPC durante o segundo semestre de 2017, em que pese a atuação quase irrelevante verificada no primeiro semestre desse mesmo ano, conforme mostrado a seguir:

- Comitê de Governança, Riscos, Controle realizou quatro reuniões (03/07/2017, 29/08/2017, 06/10/2017 e 30/10/2017);
- Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira realizou três reuniões presencias e três

plenárias virtuais, resultando na publicação de 16 resoluções.

15. Em que pese inexistência de Política de Riscos, durante o exercício de 2017, o CGRD-GD aprovou e publicou o documento em 2018, por meio da Portaria nº 40, de 20 de junho de 2018, evidenciando que a alta administração da UPC encontra-se atenta à área de gestão de riscos.

16. Além disso, foi publicada a Portaria nº 16, de 9 de fevereiro de 2018, que trata da Política de Governança de Tecnologia da Informação e Comunicação - PG TIC, e é constituída por um conjunto de objetivos, princípios, diretrizes, normas, processos, estruturas organizacionais e pessoas, visando a criação de valor para a Instituição e para o cidadão, mediante uso dos recursos de tecnologia da informação e comunicação.

17. Outrossim, vale ressaltar que o Plano Diretor de Tecnologia da Informação e Comunicações – PDTIC 2017/2018 estabeleceu metas de capacitação com objetivo de aprimoramento da força de trabalho, contudo tais metas não estão alinhadas ao Plano anual de capacitação do ITI, o que demonstra uma fragilidade do processo.

18. Impende ressaltar ainda que a UPC se utilizou de seu planejamento estratégico como referencial para construção do PDTIC, o que evidencia uma boa prática de governança de TI que visa estabelecer um alinhamento entre o plano estratégico com o tático operacional do ITI. Todavia, constatou-se que o PDTIC 2017-2018 não está alinhado com a Estratégia de Governança Digital – EGD, conforme exigência estabelecida no Decreto nº 8.638, de 15 de janeiro de 2016.

19. Em manifestação ao Relatório de Auditoria preliminar, a UPC informou que “o PDTIC atualmente vigente no âmbito do ITI (PDTIC 2017-2018), embora não tenha sido elaborado contemplando o alinhamento explícito com a EGD, abrangeu diversas ações voltadas para facilitar o acesso do cidadão aos serviços providos pela instituição, dentre as quais se destacam as contratações de serviços de contingência de conexão com a internet, os serviços de manutenção e melhoria da Autoridade Certificadora Raiz do ICP-Brasil, e a ampliação dos serviços providos pela rede INFOVIA. Todas estas ações foram executadas com êxito e trouxeram melhorias para o funcionamento da Autoridade Certificadora Raiz, que, sem dúvida, refletiram em uma melhor percepção da comunidade em relação aos serviços prestados pelo ITI” e que “a nova versão do PDTIC para os anos de 2018 e 2019, em fase de elaboração, contemplará de forma mais explícita o alinhamento com as estratégias de governo eletrônico previstas na EGD”.

20. Ademais, cumpre salientar que a UPC não apresenta alinhamento no que diz respeito aos instrumentos de Governança de TI elaborados para a AC Raiz do ICP Brasil e para a área meio de TI do ITI. Como exemplo de tal desalinhamento, pode-se mencionar a existência de um Plano de Contingência e de um Plano de Continuidade de Negócio que são específicos para a área da AC Raiz da ICP Brasil.

21. No que diz respeito à norma de Política de segurança da informação e comunicação, observa-se que a UPC possui uma norma vigente, mas que não sofre atualizações desde o exercício de 2008.

22. Quanto aos procedimentos de segurança da sala cofre da AC-Raiz-ITI, constata-se uma forte sensação de segurança do ambiente, bem como um efetivo controle por parte da diretoria responsável por sua gestão (DINFRA).

23. Além disso, a UPC pouco avançou no que diz respeito à implantação da estrutura de segurança da informação e comunicações do ITI, tais como: a) a implantação do Comitê de Segurança da Informação e Comunicações; b) a nomeação do Gestor de Segurança da informação e Comunicações; c) a instituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais– ETIR¹; e d) a designação do chefe para a ETIR.

24. Por fim, no tocante às aquisições e soluções de TI, constata-se a contratação de serviços especializados para operação de segurança da informação do ITI, bem como existência de Termo de execução descentralizada-TED não aderente à legislação de aquisições de TI.

A.II. GERENCIAMENTO DE RISCOS

25. Com o objetivo de avaliar o gerenciamento de riscos da unidade, buscou-se elencar os riscos de maior impacto e probabilidade no negócio da UPC.

26. Nesse sentido, podemos destacar os seguintes riscos: a) alteração na estrutura com alteração do órgão supervisor do ITI; b) Risco de adoção de tecnologia com falhas; e c) mudança intempestiva nos requisitos que afetam a infraestrutura de chaves públicas. Os possíveis impactos aos negócios da organização associados a esses riscos são a perda de servidores técnicos com risco de continuidade de negócio, a perda de confiança na infraestrutura de chaves públicas (ICP-Brasil) e a limitação da usabilidade dos certificados digitais emitidos pelo ICP-Brasil.

B. MECANISMOS DE GOVERNANÇA E INTEGRIDADE

27. Sob a perspectiva da governança pública, procurou-se avaliar a conformidade e eficácia dos mecanismos atualmente existentes para identificar e neutralizar as ameaças (riscos) aos principais objetivos da UPC, alinhado com as disposições do referencial de Governança do Tribunal de Contas da União (TCU) e com o Guia de Integridade Pública, elaborado pelo Ministério da Transparência e Controladoria-Geral da União (CGU).

¹ Conforme definido pela Instrução Normativa nº 01/2008, do Gabinete de Segurança Institucional da Presidência da República-GSI/PR.

28. O adequado gerenciamento dessas ameaças, por parte do gestor, deve contemplar a identificação e a análise dos alertas apresentados pelos órgãos de controle, pela sociedade e pelos mecanismos de controle já instituídos, com consequente tomada de decisão, com vistas à adoção de medidas para mitigar essas ameaças ou aceitá-las, apresentando justificativas necessárias.

29. Diante do exposto, apresenta-se a seguir os resultados da avaliação que contemplou a gestão dos seguintes mecanismos de controle:

- a. análise gerencial a respeito de compras e contratações;
- b. avaliação dos mecanismos de transparência e controle social – ouvidoria; e
- c. avaliação da gestão de pessoas.

30. Com relação à gestão de compras e contratações durante o exercício de 2017, vale ressaltar que esta Secretaria de Controle Interno realizou, de forma concomitante aos editais de licitação, a análise de dois editais de licitação (Pregão nº 5/2016 e Pregão nº 9/2016, nos montantes de R\$ 3.341.992,72 e 567.770,00, respectivamente).

31. Esses dois pregões respondem por 82,3% do total gasto com compras e contratações na unidade durante o exercício de 2017 e tiveram seus valores significativamente alterados após cumprimento de recomendações emanadas pela Ciset, conforme demonstrado na seção de Achados de Auditoria deste relatório.

32. No que diz respeito à ouvidoria, cumpre ressaltar que o Instituto Nacional de Tecnologia da Informação (ITI) não possui uma estrutura formalmente instituída para essa atribuição, em que pese a atividade constar em seu Regimento Interno, aprovado por meio da Portaria nº 20, de 28 de fevereiro de 2018.

33. Ademais, apesar de o ITI ter autonomia para dar tratamento às manifestações enviadas por meio do e-OUV, a Ouvidoria/PR faz o acompanhamento do desempenho das atividades vinculadas ao fornecimento de respostas às manifestações que são diretamente endereçadas ao Instituto.

34. Por fim, no que diz respeito à Gestão de Pessoas, vale destacar a ausência de quadro próprio de pessoal e que essa particularidade gera inúmeras dificuldades e fragilidades para o ITI, conforme discorrido na seção de Achados de Auditoria deste relatório.

C. CONCLUSÃO

35. No geral, nota-se que um dos grandes riscos do ITI está relacionado à ausência de quadro próprio de pessoal, conforme já mencionado nesse relatório e detalhado na seção de Achados de Auditoria.

36. Visando equacionar esse problema da criação de um quadro próprio e

da instituição de um Plano de Cargos e Salários, em 2013, a UPC solicitou à Casa Civil da Presidência da República, por meio do Ofício 74/2013-GAB/ITI/PR, de 23/09/2013, sua inclusão dentre as entidades autorizadas a adotar o Plano de Carreiras para a área de Ciência e Tecnologia, previsto na Lei 8.691/93.

37. Por fim, seria um grande aprimoramento da governança e gestão da tecnologia da informação caso o ITI aplicasse os mesmos planos, procedimentos e metodologias aplicadas à infraestrutura da AC Raiz do ICP-Brasil às demais áreas do TI do Instituto Nacional de Tecnologia da Informação, pois, tendo à sua disposição um arsenal de instrumentos com elevado grau de maturidade, não faz sentido não aplicá-lo a todas as áreas da UPC.

D. RECOMENDAÇÕES

38. Recomenda-se à UPC que proceda a avaliação dos achados evidenciados durante os trabalhos e elabore plano de ação contendo medidas a serem adotadas, no âmbito de cada área responsável, para eliminá-los ou reduzir seus impactos a níveis considerados aceitáveis pela própria gestão; apresentando os subsídios técnicos que suportem essa decisão.

1) Governança e gestão de Tecnologia da Informação

Governança de TI

- 1.1) Achado 1.2: Insuficiência de indicadores de desempenho e de resultado no planejamento estratégico durante o exercício de 2017.

Possíveis impactos: impossibilidade de avaliação do desempenho no que diz respeito à possibilidade de comparação de uma medida com metas preestabelecidas.

- 1.2) Achado A.I - Governança e Gestão de Tecnologia da Informação - Plano Diretor de Tecnologia da Informação e Comunicações-PDTIC não alinhado com a Estratégia de Governança Digital – EGD.

Possíveis impactos: prejuízo ao aprimoramento da prestação dos serviços pela insuficiência de alinhamento com a Política de Governança Digital-PGD e mais especificamente com a EGD vigente.

- 1.3) Achado 1.5: Ausência de processos formais de Gestão de Configuração, mudanças e riscos de TI.

Possíveis impactos: dificuldade para fornecimento de informações para outros processos dos itens de configuração – IC's acarretando desarmonia entre eles; incremento no risco de continuidade dos serviços de TI e ausência de controle da infraestrutura de TI

Aquisições e soluções de TI

- 1.4) Achado A.I – Governança e Gestão de Tecnologia da Informação: Contratação de serviços especializados para operação de segurança da informação.

Possíveis impactos: vazamento de informações sensíveis e/ou estratégicas inerentes à ICP-Brasil e ao ITI.

- 1.5) Achado A.I – Governança e Gestão de Tecnologia da Informação: Termo de execução descentralizada-TED não aderente à legislação de aquisições de TI.

Possíveis impactos: vazamento de informações sensíveis e/ou estratégicas inerentes à ICP-Brasil e ao ITI.

2) Processos de Compras e Contratações

- 2.1) Achado 3.1.1: adoção de fator k fora dos parâmetros de economicidade recomendados pela Corte de Contas.

Possíveis impactos: realização de compras antieconômicas e com prejuízo ao erário; responsabilização por descumprimento de normativos legais.

- 2.2) Achado 3.1.2: adoção de estimativa com preços superiores em relação à média de preços para equipamentos com especificações similares e previsão de compras de equipamentos em quantitativo superior à força de trabalho atual do ITI

Possíveis impactos: (i) realização de compras antieconômicas e com prejuízo ao erário; responsabilização por descumprimento de normativos legais; (ii) realização de compras desnecessárias e prejuízo ao erário; responsabilização por descumprimento de normativos legais.

3) Avaliação dos Mecanismos de Transparência e Controle Social - Ouvidoria

- 3.1) Achado 4.1.1: Ausência de área responsável pelo tratamento de demandas típicas de Ouvidoria Pública

Possíveis impactos: (i) responsabilização por descumprimento de normativos legais; (ii) Falta de universalização do serviço de ouvidoria; Possibilidade de enviesamento dos indicadores de ouvidoria e (iii) Possibilidade de classificação de informações incorreta, o que pode colocar em risco informações sigilosas e/ou estratégicas da UPC.

39. Ademais, destacamos abaixo oportunidades de melhoria ao ICP-Brasil, que fazem parte da esfera de governabilidade do Comitê Gestor do ICP-Brasil e, portanto, não estão sob a esfera de governança do ITI, conforme detalhado no Anexo de Achados de Auditoria.

40. Nesse contexto, recomenda-se que o ITI **encaminhe essas oportunidades de melhoria ao Comitê Gestor do ICP-Brasil** com sugestões de aperfeiçoamento da governança:

Mecanismos de Governança Institucional

- 7.1) Oportunidade de Melhoria: Atualização da Metodologia de desenvolvimento de software (DOC-ICP-01).

Resultado esperado: aprimoramento do processo de contratação e aferição da qualidade dos produtos entregues; desenvolvimento de *software* em linguagens e plataformas adequadas ao negócio da organização, contribuindo com a continuidade quando da incorporação do sistema pelo ITI.

- 7.2) Oportunidade de Melhoria: Atualização da Política de segurança da informação e Comunicações (DOC-ICP-02).

Resultado esperado: processos e procedimentos de gestão de TI, melhor estruturados e redução da possibilidade de incidentes de fraudes, ameaças, vulnerabilidades e até perda de dados/informação ou quebra da cadeia de confiança.

Mecanismos de Segurança da Informação e Comunicações

- 7.3) Oportunidade de melhoria: Incrementos na estrutura de segurança da informação e comunicações.

Resultado esperado: Melhoria na segurança na guarda de informações sigilosas e/ou relevantes para o negócio da unidade; incremento na confiança em toda a estrutura de chaves públicas do Brasil.

41. Por fim, **recomenda-se** que se **faça a gestão dos seguintes itens junto ao Ministério do Planejamento e à Casa Civil da Presidência da República**, conforme detalhado a seguir:

- 7.4) Oportunidade de melhoria: Estabilidade na estrutura sem alteração do órgão supervisor do ITI.

Resultado esperado: Estabilidade de servidores técnicos contribuindo com a continuidade do negócio; continuidade da sala cofre dentro do sítio da Presidência da República.

- 7.5) Oportunidade de melhoria: Criação de quadro próprio de servidores

Resultado esperado: diminuição da rotatividade da força de trabalho; continuidade do negócio e manutenção de conhecimentos relacionados à competência do ITI.

III. ACHADOS DE AUDITORIA

DO SISTEMA DE CERTIFICAÇÃO DIGITAL BRASILEIRO E A ICP-BRASIL²

1. Preliminarmente, dadas as especificidades das atividades realizadas pelo ITI enquanto Autoridade Certificadora Raiz da ICP-Brasil, faz-se necessário, antes de se adentrar propriamente nas constatações e recomendações constantes do referido Relatório de Auditoria, tecer algumas considerações gerais acerca do Sistema de Certificação Digital Brasileiro e da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, com especial destaque ao papel desempenhado pelo ITI e por cada uma das entidades integrantes. Registre-se, desde logo, que eventuais aprofundamentos que se façam pertinentes quanto a determinado ponto específico serão realizados quando da manifestação quanto ao risco e/ou recomendação concretamente enfrentada.

2. O Sistema Nacional de Certificação Digital foi instituído pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, a fim de “[...] *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*” (art. 1º).

3. Ressalte-se, desde logo, que tal Medida Provisória encontra-se em **vigor**, de acordo com a EC 32/01, art. 2º, verbis:

Art. 2º As medidas provisórias editadas em data anterior à da publicação desta emenda continuam em vigor até que medida provisória ulterior as revogue explicitamente ou até deliberação definitiva do Congresso Nacional.

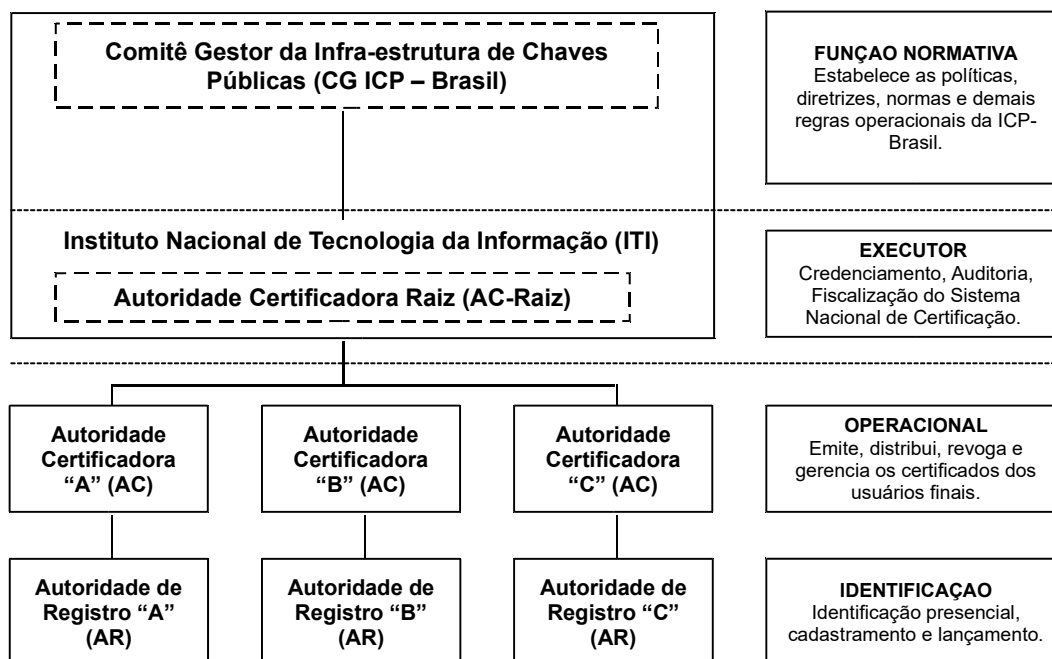
4. A infraestrutura é integrada por uma Autoridade Gestora de Políticas (o Comitê Gestor da ICP-Brasil), uma Autoridade Certificadora Raiz (o ITI), as Autoridades Certificadoras de nível subsequente ao da Raiz e as Autoridades de Registro, conforme dispõe o art. 2º da MP nº 2.200-2/01. Além destes, pode-se apontar, ainda, as entidades de apoio (Prestadores de Serviço de Suporte – PSS. Prestadores de Serviços Biométricos – PSBio, entre outras), previstas nas normas regulamentares expedidas pelo Comitê Gestor e, logicamente, os usuários de todo esse sistema, vale dizer, aqueles que se utilizam dos certificados emitidos no âmbito da ICP-Brasil.

5. A competência de cada um dos integrantes da infraestrutura encontra-se delineada MP nº 2.200-2/01, e especificada nas normas expedidas pelo Comitê Gestor.

² Informação extraída da manifestação ao Relatório de Auditoria preliminar do ITI, encaminhada à Ciset em 11/9/2018.

6. Em poucas palavras e de forma sucinta, pode-se assim resumir o papel desempenhado por cada qual na ICP-Brasil: a) o Comitê Gestor estabelece as normas; b) o ITI, as executa e fiscaliza as entidades cadastradas; c) as Autoridades Certificadoras, conforme o próprio nome diz, emitem os certificados; d) as Autoridades de Registro, que são vinculadas às Autoridades Certificadoras, identificam presencialmente os adquirentes desses certificados. As PSS e as demais entidades de apoio, por sua vez prestam serviços de apoio às demais entidades.

Gráfico 1 – Estrutura esquemática do ICP-Brasil



Fonte: Manifestação ao Relatório de Auditoria preliminar

7. Nesse contexto, o Comitê Gestor é a Autoridade Gestora de Políticas da ICP-Brasil. Significa dizer que é o órgão normativo máximo da ICP-Brasil, a quem compete, dentre outras atividades, editar as normas (infralegais) técnicas da ICP-Brasil, conforme dispõe o art. 3º e 4º, da MP nº 2.200-2/01:

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio

Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos 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 - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;

V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionais das AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar 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; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

8. Note-se que, como expressamente previsto no caput do art. 3º, o Comitê Gestor é um órgão vinculado à Casa Civil da Presidência da República, e não ao ITI. Esse é um ponto que merece destaque, porquanto, algumas atividades descritas nesse Relatório são de competência do Comitê Gestor, e não do ITI.

9. O ITI, inclusive, não possui assento no Comitê Gestor, o qual é formado por representantes de diversos segmentos do Poder Público e da sociedade civil, sob a Coordenação da própria Casa Civil da Presidência da República (art. 3º, §1º). Os únicos papéis reservados ao ITI junto ao mencionado Comitê é aquele atribuído ao seu Diretor-Presidente, a quem compete exercer a função de Secretário-Executivo e, por consequência, de Coordenador da Comissão Técnica Executiva – COTEC, e isso por força de previsão constante não da citada Medida Provisória, mas sim de ato regulamentar, qual seja, o Decreto nº 6605, de 14 de outubro de 2008 (art. 6º), que a regulamentou.

10. Essa disposição não se deu injustificadamente, tendo sua razão de ser justamente na segregação das atividades afetas a cada uma das entidades integrantes da ICP-Brasil. Como ao ITI cabe o papel de Autoridade Certificadora Raiz, como se verá a seguir, não se justificaria a sua inclusão também como membro integrante do Comitê Gestor. Não é, aliás, tecnicamente correto entender o ITI como integrante da Secretaria-Executiva, órgão este integrado, exclusivamente por seu Diretor-Presidente.

11. O Comitê Gestor – e não o ITI – é, portanto, o órgão normativo da ICP-Brasil, a quem compete a edição das normas técnicas aplicáveis à Infraestrutura. Apenas mediante delegação do próprio Comitê Gestor, conforme previsto no art. 4º, parágrafo único da MP nº 2.200-2/01, é que o ITI poderá editar atos normativos relativos à ICP-Brasil.

12. As decisões do Comitê Gestor são tomadas por meio de Resoluções (art. 2º, §4º, do Decreto nº 6.605/2008), e refletidas normativamente nos chamados DOC ICP Brasil, consolidados na forma de anexos à mencionadas resoluções. Perceba-se, assim, que os chamados DOC ICP Brasil nada mais são que consolidações das normas técnicas aprovadas pelo Comitê Gestor no exercício de sua competência normativa, a

ele atribuída diretamente pela Medida Provisória nº 2.200-2/01.

13. Perceba-se, com isso, que a competência do Comitê Gestor é própria e de todo distinta daquela desempenhada pelo ITI. Com efeito, o Instituto Nacional de Tecnologia da Informação – ITI é a Autoridade Certificadora Raiz da Infraestrutura de Chaves Públicas Brasileira³. É, portanto, a primeira autoridade da cadeia de certificação, responsável pelo credenciamento, auditoria e fiscalização das Autoridades Certificadoras de nível subsequente, das Autoridades de Registro e Prestadores de Serviço de Suporte, nos termos do art. 5º da MP nº 2.200-2/01:

14. “Art. 5º. À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subsequente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.”

15. Ser Autoridade Certificadora Raiz significa dizer que possui o certificado de nível mais alto na ICP-Brasil, que contém a chave pública correspondente à chave privada utilizada para assinar o seu próprio certificado e os certificados das Autoridades Certificadoras de nível imediatamente subsequente ao seu. É, assim, a primeira autoridade da cadeia de certificação (que se estrutura como uma cadeia hierárquica de confiança), **responsável pelo credenciamento (por delegação do Comitê Gestor), auditoria e fiscalização de todas as entidades integrantes da infraestrutura, bem como executora das políticas de certificados e normas técnicas exaradas pelo Comitê Gestor.**

16. Na qualidade de AC Raiz, **o ITI jamais emite certificados para o usuário final, apenas para as Autoridades Certificadoras de nível subsequente aos seus (chamadas de ACs de 1º nível).** Cuida-se de **expressa vedação legal**, constante do art. 5º, parágrafo único da mencionada MP 2.200-2/01, a saber:

Art. 5º. (...)

Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

17. Na verdade, a competência para emissão - e renovação, quando o caso - de certificados ao usuário final é exclusiva das **Autoridades Certificadoras**, consoante dispõe o art. 6º, **CAPUT**, da mesma Medida Provisória, **IN VERBIS**:

Art. 6º Às AC, entidades credenciadas a emitir certificados

³ Art. 13 da MP nº 2.200-2/01.

digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.

18. Repise-se que a AC Raiz, ou seja, o ITI, certifica todas essas Autoridades Certificadoras. Vale dizer, emite para elas um certificado digital que demonstrará, aos usuários, que essas Autoridades podem emitir certificados digitais no âmbito da ICP-Brasil. E, por conseguinte, atribui às assinaturas eletrônicas dos usuários os efeitos jurídicos que a Medida Provisória nº 2.200-2/01 estabelece: autenticidade, integridade e validade jurídica.

19. Essas Autoridades Certificadoras, por sua vez, servem-se de Autoridades de Registro – AR para **identificar e cadastrar presencialmente** os usuários e encaminhar às ACs as solicitações de certificado (art. 7º da MP nº 2.200-2/01)⁴. Às Autoridades de Registro, então, não cabe a emissão de certificados digitais, mas tão somente o papel intransferível de **verificar a identidade dos usuários para os quais esses certificados serão emitidos**.

20. O certificado digital nada mais é que um **documento eletrônico, emitido por uma Autoridade Certificadora, que assevera a vinculação entre uma chave pública e o titular dessa mesma chave pública**. E, para que tal simples vinculação ocorra, faz-se necessária a existência de toda essa infraestrutura que acaba de ser mencionada, a fim de garantir a validade jurídica dos documentos produzidos sob a forma digital.

21. Por tudo quanto exposto, fica claro que as atividades desempenhadas pelo ITI, ainda quando no papel de Autoridade Certificadora Raiz, não se confunde com aquelas atribuídas ao Comitê Gestor ou às demais Autoridades Certificadoras, nem consistem na própria ICP-Brasil, infraestrutura criada pela MP nº 2.200-2/01, e formada não apenas pelo ITI, mas também por diversas outras entidades, cada qual com competências e atribuições próprias e inconfundíveis.

22. Portanto os instrumentos de governança relativos a AC-Raiz da ICP Brasil emanam do Comitê Gestor e seus normativos, enquanto os instrumentos governança para a área meio de TI do ITI são definidos pelo SISP. Não sendo obrigatórios o alinhamento entre esses instrumentos. Inclusive, o escopo de auditoria referente ao selo Webtrust se aplica exclusivamente a TI finalística, enquanto AC-Raiz da ICP-Brasil, o que obriga a funcionar de forma totalmente apartada da TI área meio da autarquia.

⁴ “Art. 7º. Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações”.

1. GOVERNANÇA E GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

23. No que diz respeito à governança de tecnologia da informação do ITI, procurou-se avaliar a conformidade da estrutura organizacional e dos procedimentos internos em relação às diversas normas regulamentadoras vigentes⁵ e *frameworks*⁶ de boas práticas para TI, bem como a implementação de controles internos de tecnologia da informação e a eficácia desses controles.

24. A governança de TI⁷ é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado. O IT Governance Institute (ITGI) – organismo internacional responsável por pesquisas sobre práticas e percepções globais de governança de TI para a comunidade – estabelece que “a governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização”.

25. Pode-se afirmar que a governança de TI é uma parte da governança corporativa que, em suma, consiste no estabelecimento de um conjunto de mecanismos com o objetivo de assegurar que o uso da TI agregue valor ao negócio com riscos aceitáveis, sendo responsabilidade dos executivos e da alta administração da organização prover a estrutura e garantir uma boa governança de TI.

26. A informação é um dos principais ativos de uma organização e, portanto, a área de tecnologia da informação deve realizar um gerenciamento adequado dos riscos que possuem o potencial de afetar o negócio resguardado.

27. O adequado gerenciamento dessas ameaças, por parte do gestor, deve

⁵ Dentre elas: 1) Portaria nº 19, de 29 de maio de 2017, que dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – SISP; 2) Portaria nº 20, de 14 de junho de 2016, do Ministério do Planejamento Desenvolvimento e Gestão-MPDG; 3) Acórdão TCU nº 1.233/2012 – Plenário; 4) Normas NBR/ISO 27.005:2011, 31.000:2009, 27.001:2013, 27002:2013 e 38.500:2009; 4) Normas Complementares do Gabinete de Segurança Institucional da Presidência da República-GSI/PR.

⁶ De modo a fornecer soluções para uma família de problemas semelhantes, algumas instituições elaboram compilados de boas práticas detalhando requisitos mínimos para um projeto de software possa ter uma garantia razoável de que irá atender aos seus propósitos. Os frameworks geralmente funcionam como “receitas de bolo” de boas práticas e não vinculam as decisões dos gestores, porém cada vez mais o TCU e demais órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação – Sisp tem cobrado a aderência dos órgãos e entidades a essas melhores práticas.

Neste trabalho, focaremos nos *frameworks* do Cobit 5 (boas práticas de governança e gerenciamento empresarial de TI), ITIL v3 (gerenciamento de serviços de TI) e PMBOK.

⁷ Definição em ABNT NBR ISO/IEC 38500:2009 (item 1.6.3)

contemplar a análise das recomendações/alertas apresentados pelos órgãos de controle, pela sociedade e pelos mecanismos de controle instituídos pela própria organização, com a consequente tomada de decisão com vistas à adoção de medidas para mitigar essas ameaças; ou aceitá-las, apresentando as devidas justificativas.

28. Como ponto de partida para os trabalhos de auditoria buscou-se avaliar a implementação dos controles de TI informados no Relatório de Gestão da unidade para o exercício de 2017, bem como nas respostas a solicitações de auditoria. Além disso, buscou-se também averiguar a adoção de planos e estratégias para implementação e melhoria da governança de TI.

1.1. MECANISMOS DE GOVERNANÇA INSTITUCIONAL

29. No tocante aos mecanismos de governança institucional buscou-se averiguar se a UPC possuía, ou instituiu no exercício de 2017, as instâncias de TI recomendadas pelas normas vigentes.

30. Nesse sentido, cumpre ressaltar que o ITI dispõe de um Comitê de Governança, Riscos, Controle e Governança Digital – CGRD-GD⁸, que é responsável por deliberar sobre as demandas de Tecnologia da Informação e Comunicação – TIC apresentadas pelas diversas áreas da UPC, bem como é a instância responsável por elaborar e aprovar o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC.

31. Com a implementação do citado comitê, a UPC demonstra aderência tanto em relação à exigência de criação de um Comitê de Governança Digital – CGD, conforme positivado no Decreto nº 8.638, de 15 de janeiro de 2016, quanto em relação à exigência de criação de um Comitê de governança, gestão de riscos e controles, conforme positivado na Instrução Normativa nº 01/2016, MP/CGU de 10 de maio de 2016. Ademais, a convergência das discussões nesse comitê representa uma economia administrativa tendo em vista que os temas discutidos possuem pertinência temática.

32. O citado Comitê é composto por três integrantes da alta administração da UPC, a saber: a) o Diretor-Presidente do ITI; b) o Diretor de Infraestrutura de Chaves Públicas; e c) o Diretor de Auditoria, Fiscalização e Normatização.

33. Em 2017 o CGRD-GD, se reuniu por quatro vezes⁹ e teve como resultados: a) a instituição do Grupo de Trabalho Técnico – GTT, com vistas à implementação do disposto na Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016; b) constatação da necessidade de atualização do PDTIC; c) análise e aprovação da Política de Governança de TIC do ITI.

⁸ Instituído por meio da Portaria nº 33, de 20 de junho de 2017, em substituição ao antigo Comitê Estratégico de Tecnologia da Informação – CETI

⁹ As reuniões ocorreram em 3/7, 29/8, 6/10 e 30/10. Ou seja, todas as reuniões ocorreram após a substituição do Diretor Presidente, em 28/4/2017.

34. Em que pese o CGRD-GD não ter conseguido elaborar sua Política de Riscos durante o exercício em análise, o citado comitê avançou nessa pauta com a publicação da Portaria nº 40, de 20 de junho de 2018, que estabelece o prazo de 90 dias para a conclusão da metodologia de riscos.

35. Ademais, outro mecanismo de governança de TI, é o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira que é um órgão colegiado e com atribuição de normatização relacionada à AC Raiz-ITI, conforme já explicado anteriormente.

36. Observa-se das atas dos encontros que no primeiro semestre de 2017 não houve reunião do Comitê Gestor da ICP-Brasil. Contudo, durante o segundo semestre do citado exercício foram realizadas três reuniões presenciais e três plenárias virtuais, resultando na publicação de 16 resoluções por parte desse Comitê.

1.2. INSUFICIÊNCIA DE INDICADORES DE DESEMPENHO E DE RESULTADO NO PLANEJAMENTO ESTRATÉGICO DURANTE O EXERCÍCIO DE 2017

37. No que diz respeito ao planejamento estratégico, foi constatado que o planejamento estratégico 2015 – 2018, não possuía indicadores de desempenho e de resultado para cada objetivo definido, conforme estabelece o Acórdão nº 2308/2011, do Tribunal de Contas da União-TCU-Plenário.

38. Além disso, repise-se que o Planejamento estratégico do ITI 2015 – 2018 possui 33 (trinta e três) objetivos, sendo 29 (vinte e nove) desses deveriam ter sido monitorados durante o exercício de 2017, porém durante as análises da equipe de auditoria constatou que o número de indicadores era insuficiente e não possuíam fórmula de cálculo e indicadores de resultado, conforme verificado na Nota Técnica nº 01/2015 - GTT Indicadores – ITI, de 30/09/2015, que propôs o estabelecimento de 6 (seis) indicadores, por meio desse documento para o Planejamento Estratégico ITI 2015 – 2018.

39. Por fim, outro avanço positivo da UPC, foi a publicação da Portaria nº 16, de 9 de fevereiro de 2018, da Política de Governança de Tecnologia da Informação e Comunicação – PGTIC¹⁰. Essa portaria é constituída por um conjunto de objetivos, princípios, diretrizes, normas, processos, estruturas organizacionais e pessoas, visando a criação de valor para a Instituição e para o cidadão, mediante uso dos recursos de tecnologia da informação e comunicação.

1.3. GOVERNANÇA DE TI

40. No tocante aos processos de aprimoramento da Governança de TI buscou-se averiguar se a UPC utiliza os *frameworks* de boas práticas em sua gestão.

¹⁰ Em resposta à solicitação de auditoria nº 04/2018, vinculado ao processo SEI nº 00010.000232/2018-86, a UPC informou que durante o exercício de 2017 havia uma minuta da Política de Governança de Tecnologia da Informação e Comunicação, contudo tal informação não comprovada e constata-se que essa política foi instituída pela Portaria nº 16, de 9 de fevereiro de 2018.

41. Das análises realizadas, verificou-se foi estabelecido no inventário de necessidades do Plano Diretor de Tecnologia da Informação e Comunicações – PDTIC 2017/2018 ações de capacitação com objetivo de aprimoramento da força de trabalho. Porém, examinando referido instrumento, nota-se um desalinhamento com o Plano anual de capacitação da UPC.

42. Nesse sentido, destaca-se que por resultar de uma ação da área de gestão de pessoas objetivando identificar eventuais pontos fracos nas competências dos servidores para que possam atuar com máxima eficiência nos problemas relacionados às atribuições/competências da instituição o Plano de Anual de Capacitação deve ser utilizado como uma ferramenta norteadora do processo de capacitação em TI.

43. Destaca-se que, em novembro de 2017, o ITI capacitou 20 de seus colaboradores no Curso de Gestão por Processos objetivando mapear e aprimorar os processos de TI da instituição.

44. Além disso, em seu PDTIC 2017/2018 a UPC fez uso da ferramenta de gestão conhecida por Matriz de SWOT, com o objetivo de aprimorar a governança de TI, definindo forças e oportunidades, fraquezas e ameaças.

45. Ademais, a UPC utilizou-se de seu planejamento estratégico como referencial para construção do seu PDTIC¹¹, o que evidencia uma boa prática para o aprimoramento da governança de TI, pois faz com que o plano tático operacional esteja alinhado com o plano estratégico institucional do ITI.

1.3.1. ESTRATÉGIAS E PLANOS INSTITUCIONAIS DE TI

46. No que se refere às estratégias e planos institucionais de TI buscou-se averiguar se estão definidos e se foram adequadamente implementados no âmbito da organização.

47. Inicialmente, cumpre ressaltar que a UPC possui Planejamento Estratégico¹² para o quadriênio 2015-2018¹³, o que demonstra conformidade da UPC com o art. 6º, inciso I, e no art. 7º do Decreto-Lei 200/1967.

48. O monitoramento das metas estabelecidas no referido documento, durante o exercício de 2017, foi realizado pela Coordenação-Geral de Planejamento, Orçamento e Administração – CGPOA em conjunto com a unidade denominada

¹¹ O que pode ser comprovado pela análise no anexo I – inventário de necessidades 2017/2018, no campo coluna objetivo do PE relacionado

¹² Documento acessado em 2/9/2018 e disponível no seguinte sítio:

http://iti.gov.br/images/repositorio/institucional/planejamentoestrategico/PLANEJAMENTO_ESTRATEGICO_ITI-2015-2018-versao-beta3.pdf

¹³ Documento elaborado pelo Grupo Técnico de Trabalho – GTT designado por meio da Portaria nº 24, de 17 de outubro de 2014, publicada no Boletim Interno nº 035, de 17/10/2014.

49. Ademais, a UPC possui os seguintes planos e metodologias: a) Plano de Contingência específico para área da AC Raiz da ICP Brasil; b) Plano de Continuidade de Negócio específico para a área da AC Raiz da ICP Brasil; c) Política de Segurança da Informação e Comunicação; d) Metodologia de Desenvolvimento de software; e e) Plano de Dados Abertos – PDA¹⁴.

50. Por fim, no que se refere ao Plano Diretor de Tecnologia da Informação e Comunicação 2017/2018, além de estar alinhado com o Planejamento Estratégico 2015 – 2018, conforme já mencionado, destaca-se que foi elaborado utilizando-se a metodologia do guia de PDTI do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP.

51. Nesse sentido, observa-se que a unidade possui uma metodologia/processo de desenvolvimento de software conforme informado no subitem 6.6.1 da Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-BRASIL – DOC-ICP-01¹⁵.

52. Ademais, a UPC possui documentos de análise de riscos da AC-Raiz DINFRA-ITI, Plano de Contingência e Continuidade do Negócio da AC Raiz da ICP-Brasil e análise de riscos do Firewall DINFRA-ITI.

1.4. MECANISMOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

53. A análise procurou averiguar se os mecanismos de segurança da informação e comunicações foram estabelecidos e implementados de forma a resguardar os ativos da UPC.

54. De início, destaca-se que a UPC dispõe de uma Política de segurança da informação e comunicação, conforme detalhada na norma DOC-ICP-02¹⁶, publicada em 2008 pelo Comitê Gestor da ICP-Brasil.

55. Além disso, a UPC pouco avançou no que diz respeito à implantação da estrutura de segurança da informação e comunicações do ITI, tais como: a) a implantação do Comitê de Segurança da Informação e Comunicações; b) a nomeação do Gestor de Segurança da informação e Comunicações; c) a instituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais– ETIR¹⁷; e d) a

¹⁴ Visa atender à Política de Dados Abertos do Poder Executivo Federal.

¹⁵ Acessado em 2/9/2018 e disponível no endereço eletrônico:

http://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/DOC-ICP-01_-_versao_4.5_DPC_DA_AC_RAIZ_DA_ICP-BRASIL.pdf

¹⁶ Acesso em 2/9/2018 e disponível em:

http://www.iti.gov.br/images/repositorio/legislacao/documentos-principais/DOC-ICP-02_-_v.3.0.pdf

¹⁷ Conforme definido pela Instrução Normativa nº 01/2008, do Gabinete de Segurança Institucional da Presidência da República-GSI/PR.

designação do chefe para a ETIR.

56. Por fim, repise-se que o ITI reconheceu a necessidade de instituição de uma estrutura de segurança da informação e comunicações que sirva para toda a organização (ICP-Brasil e ITI) e que as ações para a instituição dessa estrutura serão estabelecidas formalmente durante o exercício de 2019.

1.5. AUSÊNCIA DE PROCESSOS FORMAIS DE GESTÃO DE CONFIGURAÇÃO, MUDANÇAS E RISCOS DE TI

57. Complementarmente, importa mencionar que constatou-se a ausência dos processos formais de Gestão de Configuração, mudanças e riscos de TI. A inexistência do processo de gestão de configuração pode acarretar dificuldades para o fornecimento de informações para outros processos dos itens de configuração-IC's gerando desarmonia entre eles, impactar a continuidade dos serviços de TI e ausência de controle da infraestrutura de TI. Os benefícios da formalização desse processo permitem garantir o fornecimento da TI com melhor controle sobre os itens de configuração-IC's, prover informações precisas a outros processos e criar e manter uma Base de Dados de Gerenciamento da Configuração-BDGC.

58. Ademais, cumpre destacar que a Diretoria de Infraestrutura de Chaves Públicas-DINFRA possui Manual de administração do Centro de Certificação Digital – CCD (Ambiente Seguro) da AC Raiz da ICP-Brasil, com os seguintes processos mapeados: atividades do agente de segurança do posto de recepção, atividades do agente de segurança posto de monitoração) e atividades da gestão do controle de segurança.

59. Além disso, a UPC possui um manual de gerenciamento do ambiente seguro – SIGAS, que possui um robusto procedimento de controle de acesso à sala cofre da AC-Raiz-ITI.

60. Os procedimentos de segurança da sala cofre da AC-Raiz-ITI foram averiguados por esta Equipe de Auditoria em visita realizada durante os trabalhos de campo. Nessa visita, pôde-se perceber uma forte sensação de segurança do ambiente, bem como um efetivo controle por parte por parte da diretoria responsável por sua gestão (DINFRA).

1.6. AQUISIÇÕES DE SOLUÇÕES DE TI

61. O trabalho realizado em relação às aquisições de soluções de TI buscou apurar a conformidade dos procedimentos realizados com as normas vigentes de compras e contratações de TI.

62. De início, ressalta-se que as contratações de soluções de tecnologia da informação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP deverão estar de acordo com as disposições da Instrução Normativa nº 4, de 11/09/2014, da Secretaria de Logística e Tecnologia da Informação (IN - SLTI/MP nº 4/2014) e Portaria nº 20, de 14 de junho de

2016.

63. Diante disso e com vistas à verificação da conformidade e dos riscos associados durante a fase de planejamento das contratações foram analisados dois processos (processos SEI nº 99990.000328/2017-34 e 99990.000057/2017-17).

64. Da análise do processo SEI nº 99990.000328/2017-34, constatou-se que houve a contratação de agentes externos ao quadro permanente do ITI para a execução de serviço de segurança da informação (serviço sensível à TI), o que está em desacordo à Norma Complementar nº 05, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República-GSI/PR e ao Acórdão nº 1.200/2014-Plenário-TCU, conforme explicado a seguir.

65. Conforme estabelecidos na citada norma complementar o agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR deve ser “servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta”.

66. Além disso, o Acórdão nº 1.200/2014-Plenário-TCU determina aos órgãos integrantes do SISP que no prazo de 120 dias fossem identificadas as situações de atividades sensíveis e estratégicas inerentes à TI exercidas por agentes externos ao quadro permanente de pessoal da instituição, sugerindo a substituição desses por servidores ou empregados públicos efetivos .

67. No que diz respeito ao Termo de Execução Descentralizada nº 1/2017 (processo 99990.000057/2017-17), observou-se diversas inconformidades em relação à Instrução Normativa nº 04/2014, de 11 de setembro de 2014, da Secretaria de Logística de Tecnologia da Informação – SLTI, conforme detalhado no quadro a seguir:

Quadro 1 – Inconformidades do Termo de Execução Descentralizada nº 1/2017

ITENS ANALISADO (TED Nº 01/2017)	INCONFORMIDADE ENCONTRADA
Objeto: manutenção corretiva e de aprimoramento dos sistemas de certificados digitais da ICP-Brasil.	A definição do objeto está imprecisa e apresenta-se composta por dois tipos de serviços distintos, quais sejam: “manutenção” (serviço prestado de forma contínua) e “aprimoramento” (serviço prestado de forma não contínua). “Lei nº 8.666/90, Art. 14. Nenhuma compra será feita sem a adequada caracterização de seu objeto e indicação dos recursos orçamentários para seu pagamento, sob pena de nulidade do ato e responsabilidade de quem lhe tiver dado causa.” (Grifo nosso)
Termo de referência e do plano de trabalho (da forma de execução).	A metodologia de desenvolvimento de sistemas do ITI, DOC-ICP-01, não foi vinculada ao termo de referência e plano de trabalho por meio de uma diretriz, conforme orienta o Acórdão nº 2613/2011-Plenário-TCU e IN nº 04/2014, SLTI/MP, art. 17, inciso II, alínea “b”.
Plano de trabalho (da forma de execução).	Não consta a utilização de ordens de serviço – OS, conforme orientado na alínea b, inciso I, art. 18, da IN nº 04/2014, SLTI/MP.

ITENS ANALISADO (TED Nº 01/2017)	INCONFORMIDADE ENCONTRADA
	<p>O Comitê de Governança Digital é responsável pela validação e priorização de cada software a ser desenvolvido e deve deliberar e decidir sobre sua viabilidade e desenvolvimento antes de sua contratação ou do envio da demanda à empresa contratada por meio de Ordem de Serviço.</p>
<p>Termo de referência, tabela 3 (do orçamento).</p>	<p>Ausência da adoção da métrica de Ponto de função – PF para estimativa de esforço necessário para desenvolvimento de cada item/funcionalidade e inexistência de memória de cálculo detalhada da estimativa do volume a ser contratado.</p> <p>Cumprе salientar que a equipe de planejamento da contratação deve documentar a aplicação do método adotado para o cálculo das estimativas das quantidades dos itens a contratar nos autos do processo de contratação, explicitando como os cálculos foram feitos (memorial de cálculo) página 308 do Guia de contratações de soluções de TI do TCU.</p> <p><i>“Art. 22. A estimativa de preço da contratação deverá ser realizada pelos Integrantes Administrativo e Técnico para elaboração do orçamento detalhado, composta por preços unitários e fundamentada em pesquisa no mercado, a exemplo de contratações similares, valores oficiais de referência, pesquisa junto a fornecedores ou tarifas públicas.”</i> Fonte: Instrução Normativa nº 04/2014 SLTI/MP.</p>
<p>Termo de referência (cronograma de desembolso financeiro)</p>	<p>A UPC, durante o exercício de 2017 realizou pagamento antecipado do contrato em desacordo com o Acórdão nº 1.214/2013-Plenário-TCU.</p> <p>Cabe consignar que, no âmbito da administração pública, salvo pequenas exceções, não há a figura do pagamento antecipado. Ademais, tal prática não seria razoável, pois transformaria a Administração em financiadora, a custo zero, de empresas de terceirização ao invés de contratante. Além disso, se assim o fosse, as empresas trabalhariam com risco zero, situação incompatível com as atividades da iniciativa privada, que pressupõem sempre a existência do risco do negócio.</p> <p>O pagamento somente pode ocorrer após o ateste do serviço realizado.</p>
<p>Termo de referência (vantajosidade de contratações)</p>	<p>Foi constatado pela equipe de auditoria delegação do ITI à UFSC da pesquisa de preços ao fornecedor.</p> <p>A UPC não utilizou o sistema de painel de preços disponível em http://paineldeprescos.planejamento.gov.br/.</p> <p><i>“Art. 22. A estimativa de preço da contratação deverá ser realizada pelos Integrantes Administrativo e Técnico para elaboração do orçamento detalhado, composta por preços unitários e fundamentada em pesquisa no mercado, a exemplo de contratações similares, valores oficiais de referência, pesquisa junto a fornecedores ou tarifas públicas.”</i> Fonte: Instrução Normativa nº 04/2014 SLTI/MP.</p>

ITENS ANALISADO (TED Nº 01/2017)	INCONFORMIDADE ENCONTRADA

Fonte: Análises realizadas pela Equipe de Auditoria

2. GERENCIAMENTO DE RISCOS

68. No que tange o gerenciamento de riscos que afetam as atividades sob a competência do ITI, buscou-se, dentre outras, focar na análise daquelas que a um primeiro olhar apresentam maior probabilidade de ocorrência e que, caso ocorram, apresenta um elevado risco para a UPC.

69. Nesse sentido, foram elencados junto aos próprios servidores do ITI os seguintes eventos:

- Alteração do órgão supervisor do ITI;
- Adoção de tecnologia com falhas; e
- Mudança intempestiva nos requisitos que afetam a infraestrutura: foco na área de pesquisa.

2.1. ALTERAÇÃO DO ÓRGÃO SUPERVISOR DO ITI

70. Um dos maiores riscos ao qual o ITI está exposto é o de sofrer uma mudança em relação ao órgão supervisor ao qual está vinculado sem que haja um amplo estudo de impacto que abranja a avaliação de todos os riscos envolvidos e um plano de continuidade do negócio.

71. Ocorre que, atualmente, a maioria dos servidores do ITI são requisitados de outros órgãos de Administração Pública com fundamento no artigo 2º da Lei 9007/1995, de 17 de março de 1995, que estabelece:

Art. 2º As requisições de servidores de qualquer órgão ou entidade da Administração Pública Federal **para a Presidência da República** são irrecusáveis. **(grifamos)**

72. Nesse sentido, por ser uma autarquia federal ligada a Casa Civil da Presidência da República, o ITI se utiliza dessa prerrogativa para requisitar servidores para ocupar os cargos disponíveis na unidade, tendo em vista que a UPC não tem autorização para provimento de cargos por meio de concurso público.

73. Nesse contexto, um problema poderia advir de uma mudança na estrutura de vinculação do ITI para um órgão que esteja fora da estrutura da Presidência de República, pois quase a totalidade de seus servidores possuem liberação do órgão gestor de suas carreiras para exercer atividades na Presidência da República, conforme preconizado no supracitado artigo da Lei 9007/1995.

74. Então, a priori, caso uma mudança desse nível venha a ocorrer, o ITI poderia perder quase a totalidade de seus servidores. Esse risco ainda é majorado quando se leva em consideração que as atribuições da unidade são essencialmente

técnicas e que tais competências não encontram similaridades em outros órgãos/entidades da administração pública, nem em entidades privadas.

75. Além disso, cumpre salientar que a sala cofre principal do ITI encontra-se situada dentro da área da Presidência de República e, caso tal alteração estrutural fosse realizada, deveria ser realizada uma ampla discussão para equacionar esse problema, levando-se em consideração, dentre outros, o custo de se fazer a transferência da sala cofre e de construção de um novo ambiente com todos os níveis de segurança exigidos para o armazenamento da estrutura de chaves privadas do ICP-Brasil, bem como um plano de continuidade para o período de transferência que garanta a disponibilidade atual (24 horas por 7 dias na semana - 99,99%).

76. Com efeito, somente a título de demonstração da precariedade política da vinculação do ITI à estrutura da Presidência da República, pode-se citar que a Medida Provisória nº 726, de 12 de maio de 2016, transferia a supervisão do ITI da Casa Civil para o Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC.

77. Apenas durante o processo legislativo de conversão da citada medida provisória na Lei 13.341, de 29 de setembro de 2018, é que a citada transferência foi vetada. Ou seja, o citado risco aqui levantado já foi concretizado recentemente e teve seus efeitos mitigados devido ao veto ocorrido durante a tramitação do projeto de lei.

78. Por fim, destaca-se que o órgão ao qual o Instituto Nacional de Tecnologia da Informação está vinculado pode ter influência direta na capacidade de consecução de suas competências institucionais, tendo em vista que muitas autoridades certificadoras são ministérios e entidades da própria administração, tais como a Receita Federal do Brasil, os Correios, o Serpro, o Banco do Brasil, a Caixa, etc.

79. Nesse contexto, caso o ITI venha a sofrer alteração em sua vinculação para algum órgão de menor estatura hierárquica em relação aos cadastrados como autoridades certificadoras poderá encontrar dificuldades para a realização de suas atividades de credenciamento/descredenciamento, fiscalização e auditoria, pois estaria exercendo as suas competências frente a um órgão/entidade de maior estatura dentro da Administração Pública.

2.2. ADOÇÃO DE TECNOLOGIA COM FALHAS

80. Aqui, buscou-se detalhar o tratamento ao risco dado pelo ITI em relação à possibilidade de adoção de tecnologia com falhas e gerar uma vulnerabilidade na cadeia de confiança de certificação digital.

81. A título de demonstração do poder de destruição em casos de adoção de tecnologias com falhas pode-se mencionar como exemplo a ameaça enfrentada pela Estônia, no mês de novembro de 2017¹⁸, onde cerca de 760 mil certificados

¹⁸ <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/estonia-revoga-760-mil-certificados-digitais-apos-divulgacao-de-falha.html>

digitais tiveram que ser revogados.

82. Ou seja, em um caso desses como o ocorrido na Estônia, onde cerca de 63.3% do total de certificados emitidos tiveram que ser revogados, o custo da perda de confiança dos usuários em relação à estrutura de cadeia de confiança montada é imensurável e tem efeitos muito maiores do que somente o custo dos dispositivos revogados.

83. A princípio, cumpre destacar que esse é um risco inerente ao negócio e que, portanto, não poderia ser evitado¹⁹. Sendo assim, a escolha da forma de tratamento de risco pelo ITI foi mitigar o risco através da utilização de várias soluções de *hardware* bem como processo rigoroso de homologação de dispositivos por parte do INMETRO para obtenção do Certificado de Equipamento padrão ICP-Brasil.

84. Por fim, cumpre salientar que a política de riscos deve ser atualizada constantemente e recomenda-se a própria política seja atualizada de modo a prever o acompanhamento deste risco inerente ao negócio da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

2.3. MUDANÇA INTEMPESTIVA NOS REQUISITOS QUE AFETAM A INFRAESTRUTURA

85. Por se tratar de um produto com grande risco de confiança e que, portanto, deve ser gerido de forma a garantir uma baixíssima ocorrência de falhas, existem vários fóruns internacionais de discussões que fomentam a adoção de requisitos de infraestrutura necessária para a certificação digital.

86. Uma das competências da Coordenação-Geral de Normalização e Pesquisa - CGNP/DAFN/ITI é também a de pesquisa de melhores práticas e requisitos de infraestrutura exigidos por instituições internacionais com a finalidade de implementar melhorias que visam a diminuição de ameaças à cadeia de certificação.

87. Ocorre que, atualmente, somente uma pessoa da citada coordenação está encarregada de tal atribuição e, além disso, desempenha outras tarefas, tais como a de substituto do coordenador geral.

88. Nesse contexto, é importante que a UPC avalie a conveniência e oportunidade de se alocar mais pessoas para a realização dessa atividade, bem como a possibilidade de criação de estrutura própria para a realização dessa atividade.

3. PROCESSO DE COMPRAS E CONTRATAÇÕES

89. Consoante extrações realizadas no Sistema SIASG, durante o exercício de 2017 foram homologados 18 processos de compras, totalizando um montante de

¹⁹ A única forma de evitar seria não desempenhar as suas atribuições, o que não se cogita.

R\$ 4.751.167,24, conforme discriminado na tabela a seguir:

Tabela 1: Compras e contratações realizadas em 2017.

Modalidade de Compra	Qtde de Processos	%	Valor Total Homologado	%
Pregão	10	56%	4.705.451,24	99%
Dispensa de Licitação	8	44%	45.716,00	1%
Total Geral	18	100%	4.751.167,24	100,00%

Fonte: SIASG – jun/2018.

90. Por representar 99% do valor total homologado pela UPC no exercício de 2017, realizou-se a seleção, por amostragem, de alguns editais de pregão realizados com fins de obter-se informações gerenciais a respeito dos processos de compras e contratações da unidade, conforme detalhado no tópico a seguir.

3.1. PREGÕES

91. Os editais de pregões publicados durante o exercício de 2017 foram analisados com base nos critérios de materialidade e relevância, sendo avaliada a adequabilidade dos preços; o dimensionamento dos serviços/materiais; os critérios para mensuração dos serviços; a existência de cláusulas que restringem a competitividade; a legislação aplicada; e a composição dos termos de referências.

92. Nesse sentido, foram selecionados os Pregões nº 5 e 9/2016, cujos objetos e montantes, respectivamente, foram:

- contratação de serviços terceirizados, para fins de atendimento das demandas administrativas, operacionais e auxiliares, cujo valor estimado foi de R\$ 4.114.629,08; e
- aquisição de estações de trabalho, monitores secundários e equipamentos portáteis, cujo valor estimado foi de R\$ 1.047.864,00.

93. Em análise concomitante ao processo licitatório referente ao Pregão nº 5/2016, cujo valor estimado foi de R\$ 4.114.629,08, essa Secretaria de Controle Interno averiguou que a proporção entre o custo total do trabalhador (remuneração, encargos sociais, insumos, reserva técnica, despesas operacionais / administrativas, lucro e tributos) e sua remuneração líquida variou entre 2,85 e 3,14. Ocorre que os valores recomendados para esse fator, denominado fator k, pelo TCU se encontram no intervalo de 2,5 a 2,7.

3.1.1 ADOÇÃO DE FATOR K FORA DOS PARÂMETROS DE ECONOMICIDADE RECOMENDADOS PELA CORTE DE CONTAS.

94. Nesse contexto, a adoção de fator k fora dos parâmetros de economicidade recomendados pela Corte de Contas representaria uma diferença a maior de R\$ 570.308,88 na contratação, conforme detalhado na Diligência de Auditoria nº 12/2017 que foi oportunamente encaminhada ao Gestor.

95. Após os ajustes no edital do certame em função dos parâmetros de economicidade referente ao fator K, conforme solicitado por essa Secretaria de Controle Interno, o Pregão nº 5/2016 foi realizado e a proposta vencedora foi de R\$ 3.341.992,72.

96. Ou seja, em que pese o apontamento da Ciset de estimativa superestimada em R\$ 570.308,88, o pregão foi homologado por um valor R\$ 772.636,36 inferior à estimativa inicial do edital, o que representou uma economia de 19% sobre o valor total estimado para a contratação.

97. Ademais, cumpre salientar que o Pregão nº 5/2016 responde, em valores, por 70,3% do montante total de compras e contratações homologado pelo ITI em 2017.

3.1.2 ADOÇÃO DE ESTIMATIVA COM PREÇOS SUPERIORES EM RELAÇÃO À MÉDIA DE PREÇOS PARA EQUIPAMENTOS COM ESPECIFICAÇÕES SIMILARES E PREVISÃO DE COMPRAS DE EQUIPAMENTOS EM QUANTITATIVO SUPERIOR À FORÇA DE TRABALHO ATUAL DO ITI

98. Em relação ao Pregão nº 9, no valor estimado de R\$ 1.047.864,00, verificou-se, conforme detalhado na diligência de Auditoria nº 16/2017, uma diferença a maior de aproximadamente 380 mil reais no preço estimado em relação à média de preços para equipamentos com especificações similares licitados no DF, consoante extração realizada no Portal Comprasnet. Além disso, verificou-se que o quantitativo de equipamentos previsto no item 20 do Edital estava superior a força de trabalho atual do ITI. Após a comunicação dessas fragilidades à UPC o pregão foi suspenso e permanece nesse estado até o presente momento²⁰.

99. Como alternativa o gestor procedeu a aquisição de equipamentos por intermédio de ATA de Sistema de Registro de Preços (consulta SIASG NET e manifestação ao Relatório de Auditoria preliminar), adquirindo 124 unidades (112 computadores e 14 Notebook) pelo valor total de R\$ 567.770,00, com significativa redução de quantidades e valores além da diferença apontada na Diligência.

100. Ou seja, a nova contratação realizada pelo ITI representa um percentual de 54,18% do valor estimado inicialmente, o que representa uma economia de R\$ 480.094,00 aos cofres públicos.

4. AVALIAÇÃO DOS MECANISMOS DE TRANSPARÊNCIA E CONTROLE SOCIAL - OUVIDORIA

4.1. CONTROLE SOCIAL – OUVIDORIA

101. A Ouvidoria é uma unidade das organizações que representa os

²⁰ Consulta realizada em 28/06/2018 no Portal de compras do Governo Federal

interesses, no caso da Administração Pública, dos usuários dos serviços públicos na busca de soluções definitivas e da melhoria dos referidos serviços. Nesse sentido, é um importante instrumento de governança, tanto de incentivo quanto de monitoramento das políticas públicas com propósito de assegurar que o comportamento dos dirigentes esteja alinhado com o interesse da sociedade (adaptado do conceito original do Instituto Brasileiro de Governança Corporativa).

102. O conceito de ouvidoria pública, no rol dos normativos do Poder Executivo federal, encontra-se disposto no parágrafo único do artigo 1º da Instrução Normativa nº 1, da Ouvidoria-Geral da União da Controladoria-Geral da União, de 5 de novembro de 2014, atual Ministério da Transparência e Controladoria-Geral da União (CGU):

Art. 1º As ouvidorias públicas do Poder Executivo federal deverão observar as normas estabelecidas nesta Instrução.

Parágrafo único. Considera-se ouvidoria pública federal a instância de controle e participação social responsável pelo tratamento das reclamações, solicitações, denúncias, sugestões e elogios relativos às políticas e aos serviços públicos, prestados sob qualquer forma ou regime, com vistas ao aprimoramento da gestão pública.

103. Cumpre registrar que, conforme artigo 18 do Anexo VIII da Portaria nº 7, de 14 de março de 2018, que aprova o Regimento Interno da Secretaria-Geral da Presidência da República, compete à Ouvidoria/PR supervisionar as atividades desempenhadas pelas Ouvidorias dos órgãos e entidades vinculados à Presidência da República.

4.1.1. AUSÊNCIA DE ÁREA RESPONSÁVEL PELO TRATAMENTO DE DEMANDAS TÍPICAS DE OUVIDORIA PÚBLICA

104. A Ouvidoria do Instituto Nacional de Tecnologia da Informação (ITI) não está formalmente instituída, apesar de a atividade constar em seu Regimento Interno, aprovado por meio da Portaria nº 20, de 28 de fevereiro de 2018, o que se segue.

Art. 7º À Assessoria de Comunicação compete:

[...]

VIII - registrar, classificar e controlar as demandas encaminhadas à **Ouvidoria**, utilizando sistema eletrônico para o fornecimento da resposta; (grifo nosso)

105. Para acompanhamento, de forma sistemática e organizada, das alterações dos procedimentos adotados pela unidade decorrentes das informações disponibilizadas nos canais de acesso, bem como a melhoria de serviços públicos a partir da participação social, o ITI aderiu ao Sistema de Ouvidorias do Poder Executivo Federal (e-OUV), desenvolvido pelo Ministério da Transparência e Controladoria-Geral da União (CGU), cuja finalidade é receber e tratar manifestações interpostas por usuários de serviços públicos. Os órgãos e as entidades que o utilizam, localizados nas diferentes regiões brasileiras, podem encaminhar manifestações entre si, formando

uma rede.

106. Entretanto, não houve estruturação de setor, na estrutura organizacional da autarquia, para dar tratamento às demandas recebidas via e-OUV. Em resposta à SA nº 2018/026-01, o ITI informou que há acúmulo de atribuições (Canal Centralizado – contato@iti.gov.br, e-SIC e e-OUV) e que “tal situação não permite dedicar melhor tempo para o tratamento das demandas tampouco aprofundamento nos temas correlatos”.

107. Apesar de o ITI ter autonomia para dar tratamento às manifestações enviadas por meio do e-OUV, a Ouvidoria/PR faz o acompanhamento do desempenho das atividades vinculadas ao fornecimento de respostas às manifestações que são diretamente endereçadas ao Instituto.

4.2. AVALIAÇÃO DOS MECANISMOS DE TRANSPARÊNCIA E CONTROLE SOCIAL

108. A Decisão Normativa TCU nº 161, de 1º de novembro de 2017, definiu a forma, os conteúdos e os prazos de apresentação dos relatórios de gestão referentes à prestação de contas para o exercício de 2017. O artigo 7º indicou que o relatório de gestão e as demais informações que compõem a prestação de contas devem observar a estrutura de conteúdos estabelecida no Anexo II do normativo.

109. O referido anexo apresentou a Estrutura Geral de Conteúdos dos Relatórios de Gestão, sendo que, para o item “Relacionamento com a Sociedade”, espera-se do gestor a apresentação da avaliação da estratégia, estrutura, instrumentos e canais de comunicação da unidade com os usuários de seus produtos e serviços ou cidadãos em geral.

110. Para isso, o gestor deve demonstrar a existência de estruturas que garantam canal de comunicação com o cidadão para fins de solicitações, reclamações, denúncias e sugestões, bem como de mecanismos ou procedimentos que permitam analisar a percepção da sociedade sobre os serviços prestados pela unidade e as medidas para garantir o acesso às informações.

111. Com vistas a verificar os mecanismos de transparência e controle social implantados e mantidos pelo Instituto Nacional de Tecnologia da Informação (ITI), o Tribunal de Contas da União (TCU), por meio da Portaria TCU nº 65/2018, indica, dentre outros, os seguintes aspectos a serem avaliados nesta auditoria:

- Canais de acesso do cidadão;
- Carta de serviços ao cidadão
- Aferição do grau de satisfação dos cidadãos-usuários; e
- Mecanismos de transparência das informações relevantes sobre a atuação da unidade.

112. Após análises dos mecanismos implantados e mantidos pelo ITI, esta equipe de auditoria verificou o que se segue.

4.2.1. CANAIS DE ACESSO DO CIDADÃO

113. O Relatório de Gestão do ITI registra os seguintes canais de acesso do cidadão: Serviço de Informações ao Cidadão (SIC), e-mail contato@iti.gov.br, e-OUV, além de informações constantes do Portal do ITI e na página certforum.iti.gov.br. Ademais, o Instituto possui página no Facebook e Instagram.

114. Esses canais atendem às demandas oriundas de qualquer pessoa física ou jurídica, assim como de servidores e empregados lotados no Instituto. Esta equipe de auditoria não constatou registro de ações proativas com vistas à promoção da participação social nas atividades desenvolvidas pelo ITI (internet, notícias, eventos, cartilhas etc.).

4.2.2. CARTA DE SERVIÇOS AO CIDADÃO

115. Apesar de informar em seu Relatório de Gestão que o ITI divulga a Carta de Serviços ao Cidadão, esta equipe de auditoria não a localizou no site do Instituto. Entretanto, foi constatada a divulgação dos serviços oferecidos à sociedade no Portal de Serviços do Governo Federal (<https://www.servicos.gov.br>).

116. Dessa forma, por meio do referido Portal, é possível gerar a Carta Eletrônica de Serviços do ITI, onde consta o seguinte serviço prestado pelo Instituto: credenciar-se na ICP-Brasil. Entretanto, não é possível afirmar se a informação encontra-se atualizada, considerando a resposta à Solicitação de Auditoria nº 2018/026-01, em que o Instituto afirma que não há serviços do ITI no Portal de Serviços do Governo Federal, em virtude da “minguada força de trabalho e a priorização de outras atividades não menos importantes”.

4.2.3. AFERIÇÃO DO GRAU DE SATISFAÇÃO DOS CIDADÃOS-USUÁRIOS

117. O artigo 4º, inciso II, do Decreto nº 8.936, de 19 de dezembro de 2016, determina que todos os órgãos e entidades da administração pública federal devem cadastrar e atualizar as informações dos serviços públicos oferecidos no Portal de Serviços do Governo Federal, onde há previsão de ferramenta eletrônica a ser disponibilizada para o usuário avaliar os serviços públicos prestados.

118. Nesse mesmo sentido, o Decreto nº 6.932, de 11 de agosto de 2009 também dispôs do dever dos órgãos e entidades do Poder Executivo Federal em aplicar periodicamente a pesquisa de satisfação dos usuários de seus serviços.

119. Não obstante a revogação do Decreto nº 6.932/2009, o artigo 20 do Decreto nº 9.094/2017 manteve a obrigatoriedade da utilização de ferramenta de pesquisa de satisfação dos usuários dos seus serviços, constante do Portal de Serviços do Governo Federal e do Sistema de Ouvidoria do Poder Executivo federal, e utilizar os dados como subsídio relevante para reorientar e ajustar a prestação dos serviços.

1. No Relatório de Gestão do Instituto é informado que “em virtude de limitação orçamentária, não foi possível a contratação de serviço especializado para

mensuração da satisfação dos usuários de nossos canais. Registre que o ITI opera no mesmo patamar orçamentário há mais de quatro anos, sendo que os reajustes contratuais e despesas gerais vêm sendo compensados com cortes em pessoal e investimento”.

120. Entretanto, conforme previsão do artigo 20 do Decreto nº 9.094, de 17 de julho de 2017, registra-se que, em razão de o Instituto constar no Portal de Serviços do Governo Federal, o serviço registrado poderá valer-se de pesquisa para aferir o grau de satisfação do usuário, não havendo, dessa forma, necessidade de contratação para tal fim.

4.2.4. MECANISMOS DE TRANSPARÊNCIA DAS INFORMAÇÕES RELEVANTES SOBRE A ATUAÇÃO DA UNIDADE

121. Por força da Portaria Interministerial nº 1.254, de 18 de maio de 2015, da CGU, o ITI adotou o Sistema Eletrônico do Serviço de Informações ao Cidadão (e-SIC), que permite a qualquer pessoa, física ou jurídica, encaminhar pedidos de acesso à informação, acompanhar o prazo e receber a resposta da solicitação realizada para órgãos e entidades do Poder Executivo federal.

122. Conforme dados constantes do Relatório de Gestão do ITI foram feitos 592 pedidos de acesso à informação no exercício de 2017, via Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC) e e-mail SIC. No site, há direcionamento para o Portal e-SIC, bem como consta o contato da autoridade de monitoramento responsável por verificar o cumprimento da Lei de Acesso à Informação (LAI), conforme previsão do artigo 40 da Lei nº 12.527, de 18 de novembro de 2011.

123. No site do ITI (<http://www.iti.gov.br/informacoes-classificadas>), consta publicação do Diário Oficial da União de 16 de maio de 2012 de informações classificadas como secretas. Cumpre salientar que a publicação da portaria não satisfaz a necessidade de classificação de informações, que devem formalizadas por meio de Termo de Classificação de Informação (TCI), conforme artigo 31 do Decreto nº 7.724, de 16 de maio de 2012, e modelo contido no Anexo do referido normativo.

124. No site existe link destinado à divulgação dos programas do Instituto (<http://www.iti.gov.br/programas>), mas, até a presente data, há a descrição de apenas um programa – Programa João de Barro. Quanto às despesas, há link que direciona às páginas do Portal da Transparência Pública do Ministério da Transparência e Controladoria-Geral da União.

125. Esta equipe de auditoria também verificou que consta no site a estrutura organizacional do órgão, com os respectivos ocupantes de cargos, endereço e telefone, bem como está disponível para consulta as agendas das autoridades da autarquia.

126. Esta equipe de auditoria não localizou a divulgação de dados abertos no site do ITI e no Portal Brasileiro de Dados Abertos, em inobservância ao Decreto nº 8.777, de 11 de maio de 2016, que instituiu a Política de Dados Abertos do Poder

Executivo federal.

5. AVALIAÇÃO DA GESTÃO DE PESSOAS

127. Com o objetivo de avaliar a estrutura de pessoal do ITI, sob os aspectos quantitativos e qualitativos, visando aferir sua suficiência para o cumprimento da missão institucional da Autarquia, foram promovidos levantamento de informações disponibilizadas no Relatório de Gestão, bem como a partir de manifestações da Unidade, por meio de solicitações de auditoria.

128. Inicialmente, cumpre ressaltar que a unidade não possui quadro próprio de servidores e que a sua força de trabalho é composta por 24 cargos de Direção e Assessoramento Superior (DAS) e 16 Funções Comissionadas do Poder Executivo (FCPE), conforme regulamentado no Decreto nº 8.985, de 8 de fevereiro de 2017, distribuídos entre servidores requisitados de outros órgãos e servidores nomeado sem vínculo.

129. O ITI, como órgão integrante do Sistema de Pessoal Civil da Administração Pública Federal (SIPEC), utiliza o Sistema Integrado de Administração de Pessoal (SIAPE) como ferramenta de execução e consulta de todos os dados referentes a cadastro e pagamento de pessoal. Por não possui quadro próprio, a folha de pagamento não apresenta rubricas relativas a pessoal inativo e pensionista e se compõe, basicamente, pelo pagamento do pessoal nomeado nos cargos de Direção e Assessoramento Superior (DAS).

Quadro 2 - Força de Trabalho da Unidade - Situação em 31/12/2017

Tipologia dos Cargos	Lotação
	Efetiva
1. Servidores em cargos efetivos (1.1+1.2)	55
1.1. Servidores de Carreira (1.1.1+1.1.2+1.1.3+1.1.4)	55
1.1.1. Servidores de carreira em exercício Descentralizado sem função comissionada	07
1.1.2. Servidores requisitados de outros órgãos e esferas ocupantes de Função Comissionada	24
1.1.3. Servidores requisitados de outros órgãos sem Função Comissionada	17
1.1.4 Servidores Aposentados e sem Vínculo com a Administração Pública	07
2. Servidores com Contratos Temporários	0
3. Terceirizados	77
4. Estagiários	16
5. Total (1+2+3+4)	148

Fonte: Coordenação de Auditoria Interna do ITI

130. O Quantitativo da lotação efetiva, constante no subitem 1.1.3 e 1.1.4, refere-se aos servidores requisitados de outros órgãos e sem vínculos com a

Administração Pública (ocupantes de DAS), respectivamente, conforme Decreto 8.985/2017.

131. Os sete servidores de carreira em exercício descentralizado, referem-se a Analistas de Tecnologia da Informação, lotados no quadro do Ministério do Planejamento, Orçamento e Gestão, e a dois procuradores federais, pertencentes ao quadro da Advocacia-Geral da União.

132. Ao ser questionada, por meio da Solicitação de Auditoria 2018/026-03, a respeito do quantitativo ideal de servidores para o cumprimento adequado da sua missão institucional a UPC informou que seriam necessários o acréscimo de 130 servidores, excetuando-se aqueles que já ocupavam funções comissionadas.

133. Quanto ao quantitativo de gastos com pessoal, servidores e terceirizados, foi dispendido durante o exercício de 2017, o montante de R\$ 11.029.035,38, incluindo os valores inscritos em restos a pagar no exercício de 2018, conforme apresentado no quadro abaixo:

Quadro 3 – Despesas pagas em 2017, incluindo valor inscritos em Restos a Pagar em 2018

Rubrica	Montante
Pessoal Comissionado	R\$ 2.742.741,39
Pessoal - Benefício	R\$ 82.760,79
Pessoal Requisitado	R\$ 2.742.680,47
Pessoal Terceirizado	R\$ 5.460.852,73
Total	R\$ 11.029.035,38

Fonte: Coordenação de Auditoria Interna do ITI

134. Corolário à ausência de quadro próprio de servidores o ITI também não dispõe de Plano de Cargos e Salários. A unidade opera com a mesma estrutura de cargos em comissão desde sua criação em 2002. Conforme citado anteriormente, sua estrutura de Cargos em Comissão é de 40 DAS/FCPE, ocupados por servidores requisitados da administração direta, indireta e sem vínculo.

135. Em 2013, visando a criação de um quadro próprio e a instituição de um Plano de Cargos e Salários, a UPC solicitou à Casa Civil da Presidência da República, por meio do Ofício 74/2013-GAB/ITI/PR, de 23/09/2013, sua inclusão dentre as entidades autorizadas a adotar o Plano de Carreiras para a área de Ciência e Tecnologia, previsto na Lei 8.691/93.

136. Em que pese a emissão de parecer favorável da Casa Civil, consubstanciado no Aviso nº 839/SE-C. Civil/PR, de 19/11/2013, até o presente momento não constam avanços no atendimento do pleito no âmbito do Ministério do Planejamento, Orçamento e Gestão.

137. Nesse contexto, a unidade prove as áreas para cumprimento de suas competências por meio de requisição de servidores de outros órgãos da administração

pública bem como por meio de contratação de mão de obra terceirizada para apoio administrativo, copa, limpeza, recepção, vigilância armada, etc., conforme apresentado no quadro a seguir:

Quadro 4- Contratos de Prestação de Serviços com Locação de Mão de Obra.

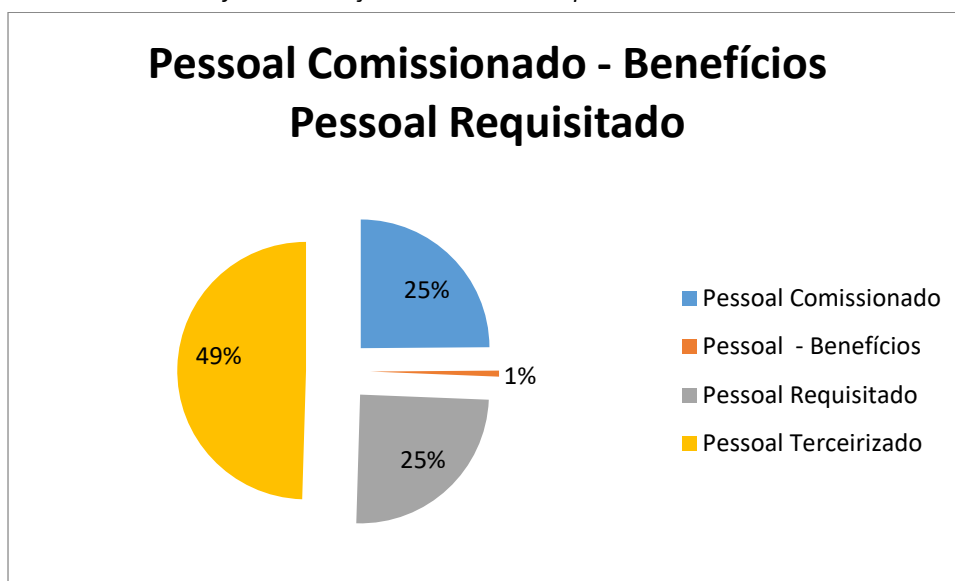
INFORMAÇÕES SOBRE OS CONTRATOS													
Nome: Instituto Nacional de Tecnologia da Informação - ITI				UG/Gestão: 243001				CNPJ: 04.039.532/0001-93					
Ano	Área	Natureza	Ident. Do Contrato	CNPJ Contratado	Per. Contratual de Exec. Das Ativ. Contratadas		Nível de Escolaridade Exigido dos Trabalhadores Contratados						Situação
					Início	Fim	Fundamental		Médio		Superior		
							Prev. no Contrato	Efet. Contratada	Prev. no Contrato	Efet. Contratada	Prev. no Contrato	Efet. Contratada	
2012	Apoio Adm.- Men. Aprendizizes	Ordinária	14/2012	13.183.890/0001-66	14/05/2012	14/05/2017	23	18	0	0	23	18	Encerrado
2012	Apoio Adm.- Men. Aprendizizes	Ordinária	13/2012	20.204.491/0001-08	14/05/2012	14/05/2017	15	9	15	9	0	0	Encerrado
2012	Apoio Adm.- Men. Aprendizizes	Ordinária	08/2012	13.183.890/0001-66	03/04/2012	03/04/2017	0	0	25	19	0	0	Encerrado
2013	Transporte	Ordinária	07/2013	20.224.491/0001-08	08/04/2013	-	5	3	0	0	0	0	Ativo Prorrogado
2013	Copeiragem	Ordinária	06/2013	20.204.491/0001-08	04/04/2013	-	4	2	4	2	0	0	Ativo Prorrogado
2013	Recepção	Ordinária	11/2013	20.204.491/0001-08	29/05/2017	-	6	2	6	2	0	0	Ativo Prorrogado
2015	Informática	Ordinária	02/2015	01.936.069/0001-94	01/07/2015	-	5	3	5	3	0	0	Ativo Prorrogado
2016	Informática	Ordinária	05/2016	02.781.209/0001-96	23/08/2016	23/08/2017	3	3	3	3	0	0	Encerrado
2017	Informática	Ordinária	08/2017	04.471.333/0001-35	24/08/2017	-	4	4	4	4	0	0	Ativo Normal
2017	Apoio Adm.- Men. Aprendizizes	Ordinária	05/2017	18.133.143/0001-37	15/05/2017	-	18	18	0	0	18	18	Ativo Prorrogado
2017	Apoio Adm.- Men. Aprendizizes	Ordinária	03/2017	20.204.491/0001-08	15/05/2017	-	7	7	7	7	0	0	Ativo Normal
2017	Apoio Adm.- Men. Aprendizizes	Ordinária	07/2017	20.204.491/0001-08	04/04/2017	-	17	17	17	17	0	0	Ativo Normal

Fonte: Controle de Contratos do ITI

138. O gasto total com contratos de terceirização no exercício de 2017 foi de R\$5.460.852,73 (cinco milhões, quatrocentos e sessenta mil, oitocentos e cinquenta e dois reais e setenta e três centavos), ou seja, 49% de toda a despesa com pessoal para o mesmo período.

139. Por se tratar de um órgão onde a informação é o principal ativo, a rotatividade usual dos empregados nos contratos de terceirização coloca em risco a continuidade do negócio, bem como a segurança de eventuais informações sigilosas do instituto. Como a unidade não possui autorização para a realização de concurso público a solução que mitigaria esse risco seria a substituição por servidores requisitados de outras órgãos.

Gráfico 2 – Relação de servidores capacitados – 2013 a 2018



Fonte: Resposta à Solicitação de Auditoria nº 2018/020-01

5.1. ASPECTOS QUANTITATIVOS E QUALITATIVOS

140. Conforme já explicado, quanto aos aspectos quantitativos, a ausência de quadro próprio prejudica significativamente o andamento das atividades da unidade, vez que os cargos de confiança são de livre nomeação e exoneração e que os terceirizados são lotados segundo critérios administrativos da contratada.

141. Quanto ao aspecto qualitativo a UPC busca suprir a carência de profissionais por meio de convênios e parcerias com outras instituições para o desenvolvimento dos projetos relacionados à sua área de atuação.

142. Da análise do planejamento estratégico 2015-2018, por meio da metodologia da Matriz de SWOT (forças, fraquezas, oportunidades e ameaças), na área de pessoal identifica-se as seguintes fragilidades:

- Estrutura organizacional defasada, tendo em 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 em muitas vezes tem alcance limitado e forte impacto nas despesas discricionárias de seu orçamento;
- Áreas críticas, como a de controle de infraestrutura de comunicação, 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 a vista sua alta disponibilidade (24 horas por dia, 7 dias por semana – 99,99%).