

RELATÓRIO

AUDITORIA NO CREDENCIAMENTO E MANUTENÇÃO DE AUTORIDADES PARA A CERTIFICAÇÃO DIGITAL

Instituto Nacional de Tecnologia da
Informação - ITI

PRESIDÊNCIA DA REPÚBLICA | SECRETARIA-GERAL
SECRETARIA DE CONTROLE INTERNO



PRESIDÊNCIA DA REPÚBLICA
SECRETARIA-GERAL
SECRETARIA DE CONTROLE INTERNO

RELATÓRIO

Auditoria no credenciamento e manutenção de
autoridades para a certificação digital

Relatório e-Aud nº 909508

Secretaria-Geral da Presidência da República
SG/PR

Missão

Assegurar a adequabilidade e a qualidade dos mecanismos de governança postos em prática para avaliar, direcionar e monitorar a gestão governamental.

Auditoria Interna Governamental

Atividade independente e objetiva de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações de uma organização. Deve buscar auxiliar as organizações públicas a realizarem seus objetivos, a partir da aplicação de uma abordagem sistemática e disciplinada para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

Qual foi o trabalho realizado pela Ciset/PRESIDÊNCIA?

Trata-se de auditoria de conformidade realizada no âmbito do Instituto Nacional de Tecnologia da Informação - ITI sobre o processo de credenciamento e manutenção de autoridades para a certificação digital.

Os trabalhos de avaliação da conformidade visam verificar se as atividades do objeto de auditoria selecionado obedecem às condições, às regras e aos regulamentos a ele aplicáveis (IN SFC/CGU nº 8/2017).

A ação de controle teve por escopo o exame da regularidade dos processos de credenciamento e manutenção de credenciamento selecionados entre os exercícios de 2017 a 2021. Analisou-se a adoção de controles internos e a implantação de medidas estruturantes na cadeia de certificação a partir de informações gerenciadas pelo ITI, especialmente com base nos dados de emissão de certificados digitais e do Cadastro de Agentes de Registro - CAR.

Por que a Ciset/PRESIDÊNCIA realizou esse trabalho?

De acordo com o art. 24 do Decreto nº 9.982/2019, compete à Secretaria de Controle Interno da Presidência da República, órgão setorial do Sistema de Controle Interno do Poder Executivo Federal, realizar auditorias na gestão dos órgãos integrantes da estrutura organizacional da Presidência da República e da Vice-Presidência da República. O Instituto Nacional de Tecnologia da Informação – ITI é uma autarquia vinculada à Casa Civil da Presidência da República.

A proposta da auditoria teve previsão no Plano Anual de Auditoria Interna – PAINT da Ciset/Presidência do exercício de 2020, e foi novamente incluída no Plano de Auditoria do exercício de 2021, a fim de contemplar a finalização dos trabalhos. A análise foi priorizada em razão da relevância do processo de credenciamento e manutenção de entidades para os resultados da Unidade examinada, sendo tema associado a objetivos previstos no Planejamento Estratégico da organização e que alcança também outros processos internos essenciais para o funcionamento das ações do ITI. A possibilidade de ocorrência de não conformidades significativas no referido processo impacta na qualidade dos serviços prestados pela Unidade e no nível de confiança que a sociedade espera para a utilização dos certificados digitais emitidos.

Quais as conclusões alcançadas pela Ciset/PRESIDÊNCIA? Quais as recomendações que deverão ser adotadas?

1. As principais conclusões em decorrência do trabalho foram:

- ✓ O processo de credenciamento de entidades, de forma geral, segue as orientações dos normativos estabelecidos pelo Comitê Gestor da ICP-Brasil;
- ✓ O processo de manutenção de credenciamento de entidades na ICP-Brasil apresenta fragilidades, por manter empresas ativas que não comprovam os requisitos de regularidade fiscal, bem como a realização de auditorias operacionais anuais;
- ✓ Insuficiência de mecanismos de gerenciamento das informações sobre o Cadastro de Agentes de Registro – CAR e sobre a emissão de certificados digitais, permitindo fragilidades como os destaques a seguir:
 - a) Agentes de Registro sem vínculo funcional comprovado com as Autoridades de Registro;
 - b) Agentes de Registro falecidos constantes do CAR;
 - c) Agentes de Registro vinculados a entidades descredenciadas ou indeferidas no CAR;
 - d) Certificados emitidos com participação de entidades com CNPJ baixado;
 - e) Certificados emitidos para titulares falecidos;
 - f) Certificados emitidos para um mesmo CPF com nomes de titulares diferentes;
 - g) Certificados emitidos com participação de Autoridade de Registro sem vínculos empregatícios na RAIS.

2. Foram recomendadas ações estruturantes em resposta às fragilidades identificadas nos controles da Unidade Auditada.

LISTA DE SIGLAS E ABREVIATURAS

AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz
AGR	Agente de Registro
ACT	Autoridade Certificadora de Tempo
AR	Autoridade de Registro
CAR	Cadastro de Agentes de Registro
CGAFI	Coordenação-Geral de Auditoria e Fiscalização
CISSET/PRESIDÊNCIA	Secretaria de Controle Interno da Presidência da República
CNPJ	Cadastro Nacional de Pessoa Jurídica
CPF	Cadastro de Pessoa Física
DAFN	Diretoria de Auditoria, Fiscalização e Normalização
DPC	Declaração de Práticas de Certificação
FGTS	Fundo de Garantia por Tempo de Serviço
GTT	Grupo de Trabalho Técnico
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
ITC	Índice de tempo médio de credenciamento
ITI	Instituto Nacional de Tecnologia da Informação
IN	Instrução Normativa
MFE	Módulo Fiscal Eletrônico
MP	Medida Provisória
PAINT	Plano Anual de Auditoria Interna
PGFN	Procuradoria-Geral da Fazenda Nacional
PLAAO	Planos Anuais de Auditoria Operacional
PR	Presidência da República
PSBio	Prestadores de Serviços Biométricos
PSC	Prestadores de Serviços de Confiança
PSCert	Prestadores de Serviço de Certificação
PSS	Prestadores de Serviço de Suporte
Quant.	Quantidade
RAIS	Relação Anual de Informações Sociais
RFB	Receita Federal do Brasil
SEI	Sistema Eletrônico de Informações

LISTA DE FIGURAS E QUADROS

FIGURAS

- Figura 1 Resumo ilustrativo da cadeia de certificação
Figura 2 Quant. de empresas credenciadas com irregularidades fiscais identificadas

QUADROS

- Quadro 1 Principais achados resultantes dos cruzamentos de dados realizados
Quadro 2 Conclusão de relatórios de auditorias operacionais
Quadro 3 Agentes de Registro sem vínculos formais na RAIS 2019 ou 2020
Quadro 4 Funcionários de serventias extrajudiciais sem vínculos na RAIS 2019 ou 2020
Quadro 5 Quant. de Agentes de Registro vinculados a entidades descredenciadas e indeferidas
Quadro 6 CNPJs mencionados no CAR não localizados na base de empresas credenciadas
Quadro 7 Certificados emitidos para titulares com registro de falecimento
Quadro 8 Exemplos de certificados emitidos para o mesmo CPF com nome do titular
Quadro 9 Exemplos de certificados emitidos do tipo “Pessoa Jurídica” com o mesmo CPF cadastrado para titulares diferentes
Quadro 10 Certificados emitidos do tipo “Pessoa Física” com o titular registrado para pessoa jurídica
Quadro 11 Certificados emitidos sem informações sobre as Autoridades de Registro (AR)
Quadro 12 Certificados emitidos com participação de AR cujo CNPJ não apresenta vínculos empregatícios na RAIS
Quadro 13 Certificados emitidos com participação de AR com indicação de menos de 2 vínculos empregatícios na RAIS, mas com quantitativo maior de Agente: Registro no CAR
Quadro 14 Certificados emitidos com participação de AR sem Agentes de Registro localizados no Cadastro de Agentes de Registro – CAR
Quadro 15 Exemplos de certificados emitidos com data futura
Quadro 16 Números de certificados emitidos com data futura (junho a dezembro de 2021)
Quadro 17 Registros de CPFs repetidos na base de dados de certificados emitidos
Quadro 18 CPFs com maiores repetições de certificados emitidos na base de dados 2020 e 2021
Quadro 19 Certificados emitidos para idosos maiores de 90 anos

SUMÁRIO

INTRODUÇÃO.....	8
RESULTADOS DOS EXAMES	14
1. Análise sobre o processo de credenciamento de entidades na ICP-Brasil.....	15
2. Análise sobre o processo de manutenção de credenciamento das entidades na ICP-Brasil.....	17
3. Manutenção do credenciamento de entidades sem o cumprimento dos requisitos de regularidade fiscal.....	18
4. Fragilidades na sistemática de controle dos Planos Anuais de Auditoria Operacional (PLAAO) e dos relatórios de auditorias operacionais.....	21
5. Análise sobre os controles internos implementados para gerenciar o cumprimento dos regulamentos da ICP-Brasil a partir do acompanhamento de dados recebidos das Autoridades Certificadoras.	24
6. Fragilidades nas informações divulgadas no Cadastro de Agentes de Registro – CAR.	24
a) Não comprovação de vínculo funcional entre 15.477 Agentes de Registro (AGR) e as respectivas Autoridades de Registro (AR) credenciadas junto à ICP-Brasil.....	25
b) Identificação de 25 Agentes de Registro falecidos, 1 menor de idade, 3 com CPFs não válidos e 4 maiores de 80 anos sem vínculo trabalhista na relação do Cadastro de Agentes de Registro – CAR.	27
c) Manutenção de 333 Agentes de Registro na base de dados do CAR com vinculação a Autoridades de Registro (AR) descredenciadas ou indeferidas.....	28
d) CNPJs de empresas mencionadas no CAR não localizados na base de empresas credenciadas na ICP-Brasil, envolvendo a vinculação de 7.099 Agentes de Registro.....	29
7. Fragilidade nos controles sobre dados de certificados digitais emitidos encaminhados pelas Autoridades Certificadoras.....	30
a) Emissão de 11.545 certificados digitais com participação de Autoridade de Registro com inscrição do CNPJ baixada.	30
b) Registro de emissão de 25 certificados digitais para titulares falecidos.....	32
c) Certificados emitidos que apresentam nomes de titulares diferentes para um mesmo CPF.....	33
d) Ausência de informações sobre as Autoridades de Registro (AR) responsáveis pelo encaminhamento de solicitações de emissão de certificados em mais de 50 mil registros.....	35
e) Certificados emitidos com atuação de Autoridades de Registro (AR) que apresentam inconsistências no assentamento dos vínculos empregatícios de Agentes de Registro.....	36
f) Certificados emitidos com data futura.....	38
g) Outras situações identificadas na base de dados de certificados emitidos.....	39
8. Informação sobre ocorrências identificadas na base de dados de certificados digitais emitidos	41
a) Multiplicidade de certificados emitidos para um mesmo CPF.....	41
b) Ausência do número de CPF do titular em 18 certificados emitidos.	42
c) Emissão de certificados para titulares maiores de 90 anos.	43
9. Falhas na divulgação de informações de interesse público no sítio eletrônico do ITI.	44

10. Informação sobre as medidas adotadas pela Unidade para atender às exigências da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.....	45
RECOMENDAÇÕES	46
ANEXO	51

INTRODUÇÃO

1. Trata-se de relatório de auditoria de conformidade que tem como objeto o processo de credenciamento e manutenção de entidades na Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. Essa auditoria decorre da previsão de ação de controle aprovada para os Planos Anuais de Auditoria Interna – PAINT da Ciset/Presidência referentes aos exercícios de 2020 e 2021.

VISÃO GERAL DO OBJETO

2. O credenciamento de entidades para prestação de serviços de certificação digital no âmbito da ICP-Brasil é um processo de relevância para o alcance dos objetivos estratégicos do Instituto Nacional de Tecnologia da Informação – ITI, autarquia federal com atribuições definidas na Medida Provisória nº 2.200-2, de 24 de agosto de 2001. O Instituto é atualmente vinculado à Casa Civil da Presidência da República, nos termos do Decreto nº 9.660, de 1º de janeiro de 2019, e tem sua estrutura regimental estabelecida no Decreto nº 8.985, de 8 de fevereiro de 2017.

3. O ITI desempenha o papel de Autoridade Certificadora Raiz – AC Raiz na Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), que é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. O modelo adotado pelo Brasil foi o de certificação com raiz única, sendo a AC Raiz a primeira autoridade da cadeia de certificação. Ela executa as políticas de certificados e as normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, além de auditar e fiscalizar as Autoridades Certificadoras – ACs, Autoridades de Registro – ARs e demais prestadores de serviços habilitados na ICP-Brasil.

4. Conforme dispõe o art. 1º da Medida Provisória – MP nº 2.200-2/01, a ICP-Brasil foi instituída para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

5. A infraestrutura é integrada por uma Autoridade Normativa – Comitê Gestor da ICP-Brasil, uma Autoridade Certificadora Raiz – AC Raiz – ITI, as Autoridades Certificadoras – AC de níveis subsequentes ao da AC Raiz e as Autoridades de Registro – AR, conforme disposição do art. 2º da MP nº 2.200-2/01. Além desses atores, destacam-se ainda as Autoridades Certificadoras de Tempo – ACT, os Prestadores de Serviço de Suporte – PSS, os Prestadores de Serviços Biométricos – PSBio e os Prestadores de Serviços de Confiança – PSC, conforme previsão em normas regulamentares emitidas pelo Comitê Gestor.

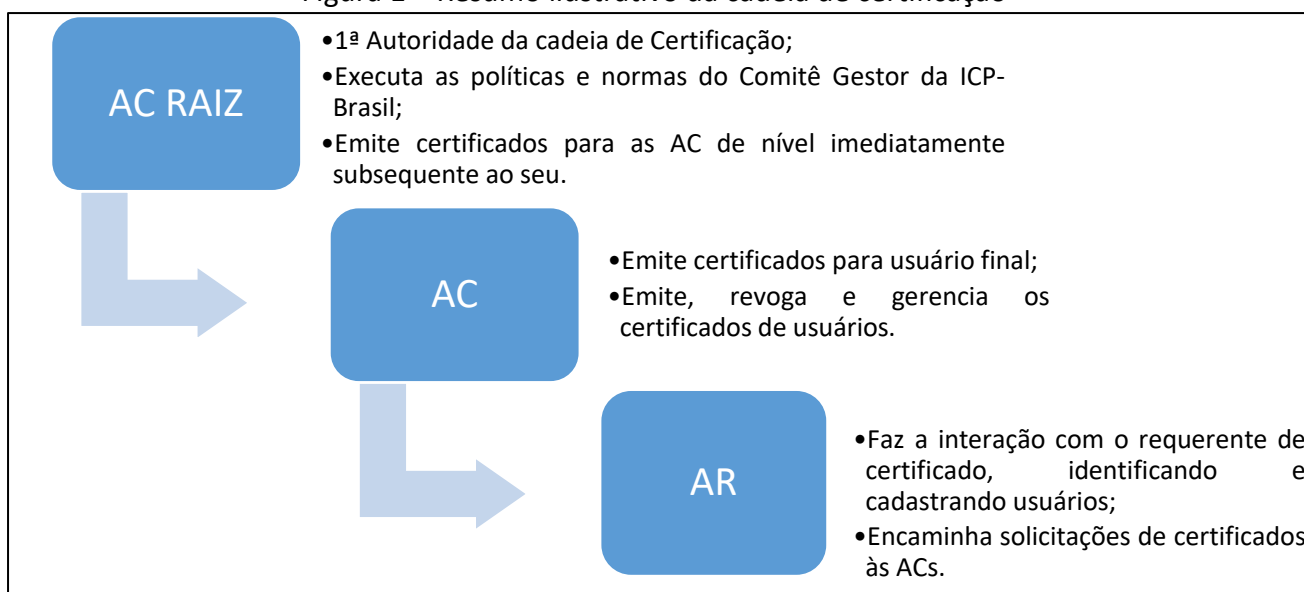
6. Em linhas gerais, o Comitê Gestor estabelece as normas, sendo o órgão regulador da ICP-Brasil. As resoluções da ICP-Brasil são organizadas em documentos principais denominados DOC-ICP, cada documento corresponde a uma resolução vigente. Ao ITI cabe executar os regulamentos editados e fiscalizar entidades habilitadas na cadeia de certificação; às Autoridades Certificadoras – AC cabe emitir os certificados; às Autoridades de Registro – AR, que são vinculadas às ACs, identificar os adquirentes de certificados; aos Prestadores de Serviço de Suporte – PSS e aos Prestadores de Serviços Biométricos – PSBio prestar serviços de apoio às demais entidades.

7. Importa destacar que o Comitê Gestor da ICP-Brasil não integra a estrutura administrativa do ITI, tratando-se de um órgão vinculado diretamente à Casa Civil da Presidência da República e composto por representantes da Administração Pública Federal e da sociedade civil, conforme estabelece o art. 3º da MP nº 2.200-2/01.

8. Como mencionado, o ITI é a Autoridade Certificadora Raiz da ICP-Brasil, sendo responsável pelo credenciamento, auditoria e fiscalização das Autoridades Certificadoras de nível subsequente, das Autoridades de Registro e dos demais prestadores de serviço habilitados na Infraestrutura. O ITI somente emite certificados às Autoridades Certificadoras de nível imediatamente subsequente ao seu – AC 1º Nível, sendo vedada a emissão de certificados ao usuário final, segundo determina o art. 5º, parágrafo único da MP nº 2.200-2/01.

9. Conforme o art. 6º da referida Medida Provisória, às Autoridades Certificadoras 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. Essas autoridades utilizam as operações das Autoridades de Registro – ARs para identificar e cadastrar presencialmente os usuários e encaminhar às ACs as solicitações de certificado. Não cabe às ARs a emissão de certificados digitais, mas tão somente o papel de verificar a identidade dos usuários para os quais os certificados serão emitidos. Um resumo dessas responsabilidades pode ser observado na figura a seguir:

Figura 1 – Resumo ilustrativo da cadeia de certificação



Fonte: Elaborado pela equipe de auditoria, conforme definições da MP nº 2.200-2/01.

10. O ITI, como consta de seu Planejamento Estratégico, tem a missão institucional de atuar na inovação, regulação e provimento de soluções tecnológicas que garantam segurança e confiança digital a documentos e transações eletrônicas. A visão declarada é ser referência nacional e internacional em tecnologias para segurança e confiança digital. Para cada objetivo estratégico foram definidos processos críticos relacionados.

11. Selecionou-se para a presente análise o processo de credenciamento de entidades no âmbito da ICP-Brasil, que está associado no planejamento da Unidade com o objetivo “Aperfeiçoar,

simplificar e consolidar o processo de credenciamento”, com previsão de indicador denominado ITC – Índice de tempo médio de credenciamento.

12. O processo de credenciamento de entidades é regulado pelo documento DOC-ICP-03, com última versão aprovada pela Resolução nº 178 do Comitê Gestor da ICP-Brasil, de 20 de outubro de 2020. É operacionalizado pela Diretoria de Auditoria, Fiscalização e Normalização – DAFN/ITI, especialmente pela Coordenação-Geral de Auditoria e Fiscalização – CGAFI, e tem os seguintes principais subprocessos de trabalho envolvidos:

- a) Solicitação de credenciamento: o candidato deverá estar em conformidade com todos os requisitos exigidos pelas resoluções do Comitê Gestor da ICP-Brasil e passará por uma auditoria pré-operacional antes do início das atividades para confirmação dos critérios requeridos. O procedimento de credenciamento obedece a dispositivos específicos, relacionados com a natureza da atividade a ser desenvolvida na ICP-Brasil;
- b) Manutenção do credenciamento: as entidades devem manter atendidos os critérios de credenciamento enquanto estiverem atuando no âmbito da ICP-Brasil. Anualmente, todos os Prestadores de Serviço de Certificação – PSCert deverão passar por auditorias operacionais para manutenção do credenciamento. Tais auditorias ocorrerão a partir do primeiro ano civil seguinte à data da publicação no DOU do credenciamento da entidade.
- c) Descredenciamento: o descredenciamento de entidades, por sua vez, ocorre diante de hipóteses previstas no DOC-ICP-03 e segue procedimentos específicos estabelecidos no referido normativo.

13. A DAFN/ITI é também a unidade responsável pela realização de auditorias, fiscalizações e revisão de normativos, entre outras competências, conforme definido no art. 24 do Regimento Interno do ITI, publicado pela Portaria nº 20, de 28 de fevereiro de 2018.

14. Convém destacar que o processo de credenciamento não abrange somente as empresas prestadoras de serviço de certificação digital, mas também as entidades de auditoria independente e os órgãos de auditoria interna que queiram realizar trabalhos de auditoria na cadeia da ICP-Brasil. Essas organizações também precisam comprovar o atendimento de critérios definidos nos normativos da ICP-Brasil a fim de conseguirem autorização para atuar.

15. Nos últimos anos, como iniciativa de melhoria no processo de credenciamento, a Unidade destacou a implementação da fila de atendimento (<https://fila.iti.gov.br>), que trouxe informações em transparência ativa sobre o andamento dos pedidos de credenciamento de entidades. Ressaltou ainda a edição da Portaria ITI nº 3, de 18 de março de 2021, que estabelece os prazos para as análises de solicitações de credenciamento na ICP-Brasil, definindo que os pedidos serão analisados pela ordem de recebimento pelo protocolo do ITI.

16. O principal sistema utilizado para cadastrar as autoridades pertencentes à ICP-Brasil é o Sistema CASA. A ferramenta possui informações relevantes para cadastro das autoridades, bem como os processos relacionados. As atividades de credenciamento, manutenção de credenciamento e descredenciamento de entidades são registradas também no Sistema SEI, servindo o Sistema CASA para consultas, atualizações e cadastramento de novas entidades e vinculações.

17. De acordo com informações da Unidade, no processo de credenciamento, o Sistema CASA é utilizado para verificar se o nome da entidade já é utilizado por algum ente da ICP-Brasil, se a empresa já foi ente da ICP-Brasil e quando deixou de ser, bem como se as vinculações solicitadas estão devidamente credenciadas. Estando tudo aderente às normas, a solicitação é deferida e a entidade é cadastrada no sistema. Na manutenção do credenciamento, o Sistema CASA é utilizado para confirmar as informações apresentadas no processo, caso esteja tudo correto e a solicitação seja deferida, o cadastro da autoridade é atualizado no sistema.

18. O Relatório de Gestão do ITI 2020 também destaca como atividades da DAFN o desenvolvimento de ferramentas para melhoria das atividades de controle e manutenção de credenciamentos. Aperfeiçoar o processo de credenciamento e fortalecer as auditorias e fiscalizações são desafios internos diretamente ligados a essa Diretoria do ITI.

19. Apenas para registro, destaca-se que, conforme previsto na política tarifária da Autoridade Certificadora Raiz da ICP-Brasil (DOC-ICP-06), a emissão de certificados pela AC Raiz, para as Autoridades Certificadoras que lhe são diretamente vinculadas, constitui serviço a ser prestado mediante a cobrança de tarifas. Na emissão do primeiro certificado de uma Autoridade Certificadora diretamente vinculada à AC Raiz, a tarifa cobrada é de R\$ 1 milhão de reais. Na emissão de certificados posteriores ao primeiro, cobra-se R\$ 200 mil. Os órgãos e entidades da Administração Pública Direta da União, dos Estados, do Distrito Federal e dos Municípios, bem como autarquias e fundações públicas, estão dispensados do pagamento das tarifas.

OBJETIVO

20. O objetivo deste trabalho foi avaliar se os procedimentos que estão em prática no âmbito do Instituto Nacional de Tecnologia da Informação (ITI) para o processo de credenciamento e manutenção de entidades seguem as determinações das normas publicadas pela ICP-Brasil, verificando possíveis diferenças entre o processo normatizado e o seu fluxo adotado no cotidiano da Unidade. Buscou-se também avaliar em que medida os controles sobre informações disponibilizadas pelas Autoridades Certificadoras estão implementados e em efetivo funcionamento, de forma a identificar o cumprimento das exigências normativas, bem como o desenvolvimento de ações para assegurar que riscos sejam geridos e os objetivos organizacionais sejam atingidos.

21. Durante o planejamento do trabalho, a equipe realizou a construção da Análise Preliminar, de forma a estudar o objeto da auditoria, com coleta de informações junto à Unidade, análise das normas aplicáveis, entre outros levantamentos, a fim de obter uma compreensão dos exames a serem executados.

22. Realizada a compreensão do objeto, a equipe definiu os objetivos do trabalho, que pretendeu responder às seguintes questões e subquestões de auditoria formuladas:

- I. O processo de credenciamento de entidades para prestação de serviços de Certificação Digital no âmbito da Infraestrutura de Chaves Pública Brasileira – ICP-Brasil tem observado os critérios e procedimentos estabelecidos no DOC-ICP-03?
 - a) As auditorias pré-operacionais estão sendo realizadas para aferir o cumprimento das exigências para credenciamento de entidades constantes no DOC-ICP-03?

- b) A instrução dos processos relativos ao credenciamento de entidades prestadoras de serviço de certificação tem observado as exigências do DOC-ICP-03?
 - c) O deferimento ou indeferimento do credenciamento é precedido de análises técnicas e jurídicas conclusivas do ITI sobre o atendimento às condições do DOC-ICP-03?
 - II. As operações para manutenção do credenciamento das entidades autorizadas a desenvolver atividades junto à ICP-Brasil (auditorias operacionais) têm observado os critérios estabelecidos no DOC-ICP-03 e no DOC-ICP-08?
 - a) As auditorias operacionais estão sendo suficientes para verificar os requisitos necessários para manutenção do credenciamento de entidades na ICP-Brasil?
 - b) As empresas que realizam auditorias estão devidamente qualificadas para realizar trabalhos na cadeia da ICP-Brasil?
 - c) Existem entidades que continuam operando na cadeia da ICP-Brasil sem a comprovação da realização das auditorias operacionais?
 - d) O ITI acompanha a regularização das não conformidades identificadas em relatórios de auditoria operacional e que ensejaram recomendações à entidade auditada?
 - III. O ITI utiliza informações relevantes encaminhadas pelas entidades da cadeia de certificação para apoiar o funcionamento dos controles internos da gestão?
 - a) O Cadastro de Agente de Registro – CAR representa fonte confiável para obtenção de informações atualizadas sobre os Agentes de Registro que podem ter acesso aos sistemas de emissão de certificados digitais?
 - b) São desenvolvidas atividades de controle pelo ITI sobre as informações de emissões de certificados digitais encaminhadas em cumprimento à Instrução Normativa nº 5, de 16 de julho de 2019?
 - IV. O ITI tem adotado medidas para atender aos requisitos estabelecidos pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)?
23. Definidas as questões de auditoria, a equipe identificou testes, critérios, informações a serem requeridas, fontes de informação, possíveis achados, e demais itens incorporados à Matriz de Planejamento do trabalho.
24. Realizou-se reunião de apresentação dos trabalhos no dia 8 de dezembro de 2020, ocasião na qual foram demonstrados à direção da Unidade os objetivos da auditoria. Durante a fase de execução, foram agendadas reuniões virtuais com a equipe da Diretoria de Auditoria, Fiscalização e Normalização, área responsável pelo processo auditado. De forma adicional, coletaram-se informações e manifestações da Unidade por meio de solicitações de auditoria encaminhadas. Os trabalhos de campo foram finalizados em junho de 2021.
25. As amostras de processos analisadas tiveram como foco o período compreendido entre 2017 a maio de 2021, considerando a disponibilização de informações no Sistema Eletrônico de Informações – SEI. As conclusões obtidas a partir da amostragem utilizada restringem-se aos itens observados nos processos analisados.

26. Em razão das restrições impostas pelo estado e emergência de saúde pública decorrente do coronavírus (COVID-19), os trabalhos foram desenvolvidos de forma remota. A situação impediu um contato mais próximo com os servidores da Unidade diretamente envolvidos com o conteúdo das análises, entretanto os recursos tecnológicos disponíveis mitigaram as dificuldades enfrentadas pelas circunstâncias do momento.

27. A estrutura principal deste relatório é composta pelos tópicos Resultados dos Exames, Recomendações e Conclusão, além desta parte introdutória. O tópico Resultados dos Exames é composto por um quadro resumo dos principais Achados de Auditoria identificados a partir dos cruzamentos de dados realizados e os demais itens estão dispostos da seguinte forma:

- a) Achados nº 1, 2 e 5: trazem informações contextuais relevantes para compreensão dos temas tratados no trabalho, abordando uma análise gerencial sobre os assuntos analisados;
- b) Achados nº 3, 4, 6 a 10: tratam dos apontamentos específicos em resposta às questões de auditoria previamente formuladas.

28. As análises dos achados e os comentários dos gestores compõem o Anexo deste relatório. Os achados de auditoria foram baseados nos processos analisados e nos cruzamentos de dados realizados, que compreenderam informações fornecidas pelo ITI e dados disponíveis em bases de sistemas governamentais. Os achados foram analisados juntamente com a sistemática de controle adotada pela Unidade, a fim de verificar o cumprimento efetivo dos regulamentos aplicáveis e indicar possíveis melhorias nas operações da organização.

29. A unidade examinada não impôs qualquer restrição à presente auditoria.

30. Espera-se que a implementação das medidas propostas nas recomendações deste trabalho possa auxiliar na melhoria de controles preventivos do ITI, aprimorando rotinas de verificações para apoiar as atividades de auditoria e fiscalização da organização, de forma a assegurar o cumprimento das regulações aplicáveis e limitar a ocorrência de inconformidades na cadeia de certificação digital.

RESULTADOS DOS EXAMES

31. Inicialmente, apresenta-se a seguir quadro gerencial com destaque para as principais ocorrências identificadas durante a execução dos trabalhos, especialmente durante as análises e cruzamentos de dados realizados a partir de amostras aplicadas, situações que serão tratadas nos itens específicos deste tópico do relatório.

Quadro 1 – Principais achados resultantes dos cruzamentos de dados realizados

Manutenção do Credenciamento	
Descumprimento dos requisitos de regularidade fiscal (Dívida Ativa, FGTS e Previdência)	100 entidades constantes da base de credenciados
Cadastro de Agentes de Registro – CAR (Base de dados 2021)	
Agentes de Registro cadastrados sem vínculo funcional comprovado	17.417 Agentes de Registro
Agentes de Registro Falecidos	25 Agentes de Registro
Agente de Registro menor de idade (7 anos)	1 Agente de Registro
Agentes de Registro com idade acima de 80 anos e sem vínculo trabalhista	4 Agentes de Registro
Agentes de Registro com CPF não encontrado na base da Receita Federal	3 Agentes de Registro
Agentes de Registro vinculados a entidades descredenciadas ou indeferidas	333 Agentes de Registro
Agentes de Registro vinculados a entidades não localizadas na base de dados de empresas credenciadas da ICP-Brasil	7.099 Agentes de Registro
Certificados digitais emitidos (Base de dados – 2020 e 2021)	
Emissão de certificados com participação de entidades com CNPJ baixado	11.545 certificados emitidos
Emissão de certificados para titulares falecidos	25 certificados emitidos
Certificados ativos com titulares que apresentam registro de falecimento	337 certificados ativos
Emissão de certificados para um mesmo CPF com nomes de titulares diferentes	789 certificados emitidos
Emissão de certificados sem identificação da Autoridade de Registro	51.201 certificados emitidos
Emissão de certificados com participação de Autoridade de Registro sem vínculos empregatícios na RAIS	130.934 certificados emitidos
Emissão de certificados com participação de Autoridade de Registro com menos de 2 vínculos empregatícios na RAIS e com quantitativo maior de Agentes de Registros indicados no Cadastro de Agentes de Registro – CAR	170.932 certificados emitidos
Emissão de certificados com participação de Autoridade de Registro sem Agentes de Registro localizados no Cadastro de Agentes de Registro – CAR	91.863 certificados emitidos

Fonte: Elaborado pela equipe de auditoria, a partir dos cruzamentos de dados realizados.

32. Importante destacar que as situações identificadas nos cruzamentos de dados devem passar por procedimentos de checagem complementar pelo ITI, a fim de que os alertas gerados possam ser validados e ações estruturantes sejam adotadas pela Unidade. Independente dos números resultantes dos cruzamentos efetuados, a Unidade deve ponderar o aprimoramento de mecanismos de controle para o cumprimento dos normativos da ICP-Brasil e a segurança do processo de certificação digital.

33. Os achados apresentados a seguir respondem às questões de auditoria elaboradas na fase de planejamento deste trabalho.

CREDENCIAMENTO DE ENTIDADES

1. Análise sobre o processo de credenciamento de entidades na ICP-Brasil.

34. O objetivo da verificação foi avaliar se os processos de credenciamento se encontravam em conformidade com as normas da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, em especial com as determinações previstas no DOC-ICP-03, que estabelece os critérios e procedimentos a serem observados para o credenciamento, manutenção do credenciamento e descredenciamento de Autoridades Certificadoras (AC), de Autoridades de Registro (AR), de Autoridades de Carimbo do Tempo (ACT), de Prestadores de Serviço de Suporte (PSS), de Prestadores de Serviço Biométrico (PSBio) e de Prestadores de Serviço de Confiança (PSC) de Assinatura Digital e Armazenamento de Chaves Criptográficas no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.

35. Para consecução desse propósito, foram selecionados processos de credenciamento de Autoridades Certificadoras de 1º Nível, Autoridades Certificadoras de 2º Nível, Autoridades de Registro, Prestadores de Serviço de Suporte e Autoridades de Carimbo do Tempo para análise.

36. Observou-se a realização de auditorias pré-operacionais antes do início das atividades dos candidatos a Prestadores de Serviço de Certificação (PSCert), em atendimento aos procedimentos para realização de auditorias dispostos no DOC-ICP-08. Verificou-se que o ITI solicita documentos complementares, quando necessário, confere os itens do DOC-ICP-03 e indefere pedidos quando o candidato não adota providências para a regularização dos requisitos exigidos pelos normativos aplicáveis.

37. Diante das amostras realizadas, verificou-se que os processos analisados apresentam conformidade com os critérios exigidos no DOC-ICP-03, apresentando uma adequada instrução. Apenas algumas falhas formais foram observadas, como a ausência de comprovação nos autos de publicações dos pedidos de credenciamento indeferidos. Entretanto, a efetiva publicação pode ser confirmada por meio de pesquisa no Diário Oficial da União (Processos nº: 00100.000584.2018/22 e 00100.001189/2020-81).

38. No exame do Processo nº 00100.006261/2019-23 (ACT IMESP), inicialmente não foi encontrada a apólice de contrato de seguro de responsabilidade civil decorrente das atividades de emissão de carimbo do tempo, com cobertura suficiente e compatível com o risco dessa atividade, conforme determina o item 2.2.4.3.2 do documento “Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil – DOC-ICP-03”. Em manifestação após o relatório preliminar, o ITI informou que a ACT IMESP enviou a apólice, conforme determina o normativo, mas, por erro, não foi anexado ao processo de credenciamento. Informou que a apólice se encontra no Processo nº 00100.000876/2021-61, situação que foi conferida pela equipe de auditoria.

39. Os processos são precedidos de pareceres técnicos com a conferência dos itens previstos nos normativos aplicáveis, fundamentando a decisão para o credenciamento ou indeferimento da entidade candidata. Em razão de últimas alterações nas exigências normativas, não é mais

necessário o encaminhamento das solicitações para análise jurídica da Procuradoria Federal Especializada/ITI.

40. Segundo informações da Unidade, o processo de credenciamento das autoridades integrantes da ICP-Brasil sofria críticas pela demora na análise e conclusão. Como forma de otimizar as análises, houve mudança nos fluxos internos do processo, que não são mais encaminhados para a análise jurídica da Procuradoria e chegam direto para avaliação da Coordenação-Geral de Auditoria e Fiscalização – CGAFI. A alteração normativa foi promovida pela Resolução do CG/ICP-Brasil nº 151/2019, que teve por objetivo a simplificação de processos na ICP-Brasil.

41. As entidades de auditoria independente candidatas a realizar trabalhos de auditoria na cadeia da ICP-Brasil também precisam cumprir os requisitos para serem devidamente credenciadas, conforme os termos do DOC-ICP-08.

42. Analisaram-se processos de credenciamento de empresas de auditoria independente para aferir a conformidade com as exigências determinadas pelo DOC-ICP-08. Em linhas gerais, os processos seguem os padrões e orientações das normas técnicas, credenciando empresas com as qualificações estabelecidas pelos normativos. Entretanto, verificou-se no credenciamento de uma empresa de auditoria independente a ausência de documentação referente ao rol de trabalhos realizados e à comprovação da experiência do corpo técnico de auditores. Após o relatório preliminar, a Unidade apresentou os documentos pendentes, os quais foram anexados ao Processo nº 00100.002199/2020-34.

43. Convém mencionar também, por oportuno, que o ITI não dispõe de informações sistematizadas e padronizadas sobre processos de trabalho importantes para a gestão que poderiam contar com um acompanhamento mais gerencial. Como exemplo, pode-se destacar não haver rotina de registro em sistemas sobre os motivos que levaram a descredenciamentos, indeferimentos de credenciamento, fiscalizações realizadas, de forma a obter com agilidade informações gerenciais dos processos de trabalho controlados. Para atender respostas das solicitações de auditoria encaminhadas pela equipe, a Unidade precisou acessar processos individuais no Sistema SEI para coletar dados e formatar planilhas.

44. A inclusão dessas informações em sistemas informatizados, atendendo a padrões a serem recepcionados pelo sistema, poderia auxiliar no tratamento dos dados e nas possíveis orientações centralizadas em resposta a fragilidades encontradas nos processos de trabalho. A sistematização das informações, até mesmo diante do aprimoramento do Sistema CASA, e a padronização de formatos dos dados a serem inseridos no sistema, poderiam evitar o controle manual por meio de planilhas, facilitar a pesquisa de informações e contribuir para a implementação de providências estruturantes a todas as entidades que compõem a ICP-Brasil. A medida indicada pode inclusive ser estendida para outros processos de trabalho de interesse da Unidade.

MANUTENÇÃO DO CREDENCIAMENTO DE ENTIDADES

2. Análise sobre o processo de manutenção de credenciamento das entidades na ICP-Brasil.

45. Conforme estabelece o DOC-ICP-03, as entidades deverão manter atendidos os critérios de credenciamento para permanecerem na estrutura da ICP-Brasil. Para evidenciar a manutenção das exigências, as entidades devem ser avaliadas anualmente por auditorias operacionais, em observância ao DOC-ICP-08. As auditorias na cadeia ICP-Brasil são realizadas pelo Comitê Gestor da ICP-Brasil, pelo ITI ou por auditorias independentes, a depender do tipo de entidade credenciada, conforme definido no item 3 do DOC-ICP-08.

46. Quanto à suficiência das auditorias operacionais para verificação dos requisitos de manutenção de credenciamento, considerando o resultado de cruzamentos de bases de dados, importa destacar os registros de empresas credenciadas que não cumprem a exigência de manutenção da regularidade fiscal, constantes do Achado nº 3.

47. No que diz respeito à realização das auditorias operacionais, verificaram-se fragilidades no controle adotado pelo ITI para acompanhamento, não sendo possível confirmar a realização de todas as auditorias necessárias, conforme relatado no Achado nº 4.

48. Em relação aos controles da AC Raiz sobre as não conformidades apresentadas em relatórios de auditoria dos PSCert, importante consignar a manifestação da Unidade apresentada no Despacho nº 0489960/2021/CGAFI/DAFN. O ITI informa que nos casos de apontamento de alguma impropriedade por empresa de auditoria independente, de acordo com o DOC-ICP-08, cabe à entidade auditada cumprir, no prazo estipulado no relatório de auditoria, as recomendações para corrigir as não conformidades identificadas. As regularizações serão comunicadas formalmente à entidade a que se vincula o PSCert auditado, na data de vencimento do prazo concedido no relatório de auditoria.

49. Conforme estabelecem os termos do item 9 do DOC-ICP-08, à entidade subordinante do PSCert cabe controlar o cumprimento das recomendações de auditoria das entidades vinculadas, comunicando ao ITI o não cumprimento de recomendações. E cabe à AC Raiz tomar todas as medidas cabíveis para garantir a segurança e a confiabilidade da ICP-Brasil, podendo descredenciar a entidade auditada, mediante decisão fundamentada.

50. De acordo com esclarecimentos do ITI, nos casos de auditorias que apresentem resultados com Conceitos 2 (Aceitável) e 3 (Deficiente), o controle das recomendações é exercido pela AC vinculada à AR auditada. Já para as auditorias com o Conceito 4 (Inadequado) ou 5 (Inaceitável), abre-se no ITI um processo para apuração e acompanhamento das não conformidades identificadas, podendo ou não ter aplicação de penalidade, após contraditório e ampla defesa.

51. Se a entidade auditada receber Conceito 5 (Inaceitável), conforme estabelece o item 9.9 do DOC-ICP-08, o ITI suspenderá imediatamente suas operações até que as não conformidades sejam solucionadas. Caso o Conceito 5 seja atribuído em duas auditorias operacionais consecutivas, poderá a entidade ser descredenciada da ICP-Brasil.

52. Conforme esclarecido, o acompanhamento realizado pelo ITI é mais voltado aos relatórios que possuem não conformidades com avaliação de riscos considerada mais crítica. Apesar disso, ainda se observou na amostra de auditoria realizada caso de empresa que recebeu Conceito 5 (Inaceitável) em relatório de auditoria operacional, mas que o ITI não iniciou processo de apuração na época devida, permitindo a operacionalização da entidade sem a observação dos critérios exigidos na legislação aplicável, conforme mencionado no Achado nº 4.

53. Nesse sentido, a manutenção das condições originais de credenciamento das entidades é fundamental para garantir a estabilidade da relação entre as partes integrantes da cadeia de certificação, confirmando a capacidade técnica em atender aos requisitos de segurança estabelecidos pelo Comitê Gestor da ICP-Brasil. Por isso, a necessidade do constante controle dos critérios exigidos nos normativos. Segundo posicionamento do ITI em respostas aos questionamentos da equipe de auditoria, se uma empresa está em conformidade com as declarações de práticas, políticas, resoluções e normas gerais estabelecidas para as entidades integrantes da ICP-Brasil apresenta capacidade para assumir os compromissos exigidos na atuação da cadeia de certificação.

54. No entanto, conforme verificado, há falhas no controle do processo de manutenção de credenciamento e na verificação do cumprimento dos requisitos normativos, o que interfere na aplicação de medidas saneadoras e impacta na capacidade fiscalizatória do ITI.

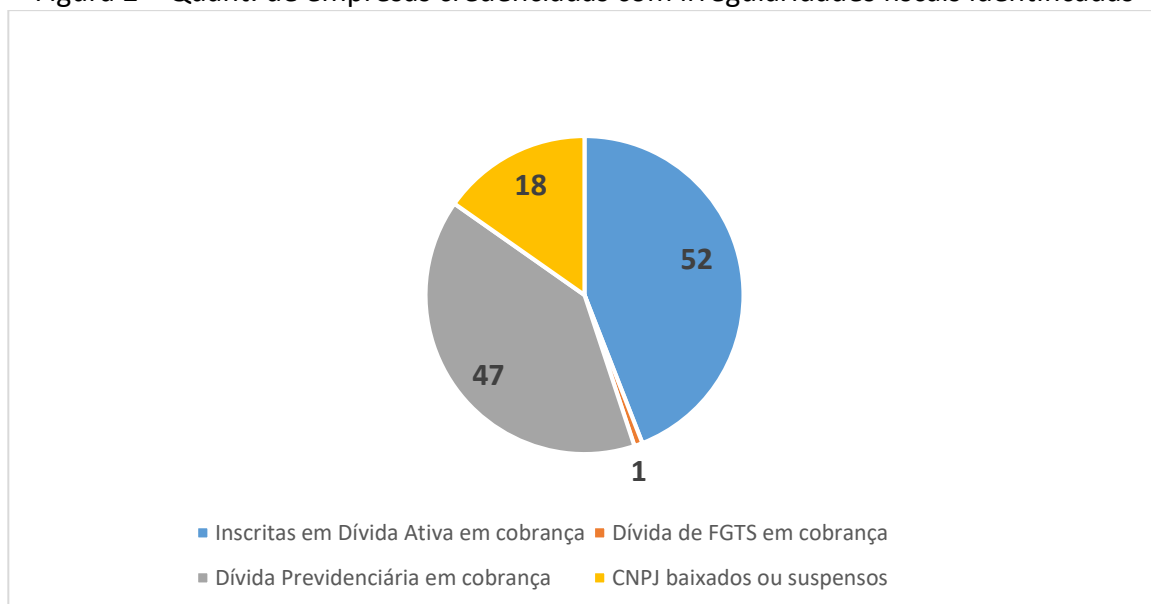
3. Manutenção do credenciamento de entidades sem o cumprimento dos requisitos de regularidade fiscal.

55. Conforme determina o item 3 do documento DOC-ICP-03 – Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil, as entidades credenciadas deverão manter atendidos os critérios definidos no item 2.1 do normativo, que define a exigência de comprovação da regularidade fiscal, com a demonstração de quitação de todas as obrigações tributárias e os encargos sociais instituídos por lei.

56. Realizados cruzamentos entre dados disponíveis em sistemas governamentais e informações cadastrais encaminhadas pelo ITI, verificaram-se as seguintes pendências:

- a) Autoridades credenciadas inscritas em Dívida Ativa em cobrança (52 empresas);
- b) Autoridade credenciada com dívida de FGTS em cobrança (1 empresa);
- c) Autoridades credenciadas com dívida previdenciária em cobrança (47 empresas);
- d) Autoridades credenciadas com CNPJs baixados ou suspensos (18 empresas).

Figura 2 – Quant. de empresas credenciadas com irregularidades fiscais identificadas



Fonte: Elaborado pela equipe de auditoria a partir do resultado de cruzamento de dados.

57. Verificou-se também em lista de devedores da Procuradoria-Geral da Fazenda Nacional (PGFN) a situação fiscal de entidades recentemente credenciadas (final de 2020 até abril de 2021), identificando ainda quatro empresas com inscrição em dívida ativa.

58. Conforme o documento ADE-ICP-08-E, que detalha os processos que compõem a cadeia de certificação e devem nortear as auditorias realizadas na cadeia da ICP-Brasil, a manutenção das condições relativas à regularidade fiscal faz parte dos itens a serem avaliados anualmente para manutenção do credenciamento de entidades.

59. Em manifestação ao achado, a Unidade apresentou o que adiante segue: “quanto ao cruzamento de dados efetivado por essa equipe de auditoria da Ciset informamos que estamos em fase de apuração pormenorizada dos fatos. Inicialmente, levantamos os Relatórios de Auditorias Operacionais/2020-2021 realizadas por empresas de auditoria independentes credenciadas pelo ITI, nas entidades citadas com supostas pendências. Em cada um dos Relatórios será verificado se os auditores independentes fizeram algum registro sobre as inconsistências descritas no cruzamento de dados. Passada esta fase oficiaremos as empresas de auditoria independentes, se for o caso, a apresentar papéis de trabalho e informações complementares sobre as pendências. A seguir, por intermédio da AC hierarquicamente superior, oficiaremos as entidades a se manifestarem sobre os apontamentos, em atendimento ao princípio constitucional da ampla defesa e do contraditório. Diante dos apontamentos constantes dos Relatórios de Auditorias Operacionais e das manifestações das entidades envolvidas, o ITI adotará providências subsequentes, caso a caso, podendo inclusive imputar penalidades e até determinar o descredenciamento de entidades, se julgar adequado. Essas serão as providências pontuais a serem adotadas nos casos descritos pela Ciset, no entanto, para as situações futuras o ITI estudará a melhor forma para adoção de rotinas periódicas para subsidiar a atuação das entidades responsáveis pela realização das Auditorias Operacionais Anuais nos PSCert, no que diz respeito à exigência de comprovação da regularidade fiscal, com a demonstração de quitação de todas as obrigações tributárias e os encargos sociais instituídos por lei”.

60. Analisou-se uma amostra de relatórios de auditorias operacionais realizadas pelas empresas de auditoria independente, sendo a seleção realizada a partir dos PSCert que apareceram em algumas das inconsistências identificadas nos cruzamentos de dados executados pela equipe de auditoria, conforme se observa a seguir:

Quadro 2 – Conclusão de relatórios de auditorias operacionais

Entidade	Tipologia do Cruzamento de dados	Ano do relatório	Conclusão do Relatório
AR Pronova	Dívida Ativa em cobrança	Janeiro de 2019	Não menciona problemas com a regularidade fiscal da empresa. Conceito do relatório é ADEQUADO.
		Fevereiro de 2020	Não menciona problemas com a regularidade fiscal da empresa. Conceito do relatório é ACEITÁVEL.
AR Projjecto	Dívida Ativa em cobrança	Janeiro de 2020	Menciona pendências com a regularidade fiscal (p. 12). Conceito do relatório é ACEITÁVEL.
		Janeiro de 2021	Não menciona problemas com a regularidade fiscal da empresa. Conceito do relatório é ADEQUADO.
		Março de 2021	Menciona pendências com a regularidade fiscal (p. 12). Conceito do relatório é ACEITÁVEL.
AR Focco	FGTS em cobrança	Setembro de 2019	Não menciona problemas com a regularidade fiscal da empresa. Conceito do relatório ACEITÁVEL.
		Outubro de 2020	Menciona não conformidade com o item 4.1.2.4.e do DOC-ICP-05 (Segurança da AR e princípios e critérios WebTrust). Conceito do relatório é ACEITÁVEL.
AR VBAM	Dívida Previdenciária	Outubro de 2019	Menciona problemas com a regularidade fiscal (p. 41 do relatório). Conceito do relatório é ACEITÁVEL.
		Outubro de 2020	Menciona não conformidade com o item 4.1.2.4.e do DOC-ICP-05 (Segurança da AR e princípios e critérios WebTrust). Conceito do relatório é ACEITÁVEL.
AR Forte Velho	Dívida Previdenciária	Setembro de 2019	Menciona problemas com a regularidade fiscal (p. 42 do relatório). Não apresentação de certidões negativas). Conceito do relatório DEFICIENTE.
		Dezembro de 2020	Não menciona problemas com a regularidade fiscal da empresa. Conceito do relatório é ACEITÁVEL.
AR Odlevati	CNPJ Baixado	Julho de 2018	Conceito do relatório é DEFICIENTE, em virtude de problemas com a identificação de solicitante (presencial).
		Agosto de 2020	Menciona não conformidade com o item 4.1.2.4.e do DOC-ICP-05 (Segurança da AR e princípios e critérios WebTrust). Conceito do relatório é ACEITÁVEL.
AR Facilita Certificado Digital	Agentes de Registro sem vínculos formais na RAIS	Dezembro de 2019	Não menciona problemas com Agentes de Registro. Conceito do relatório é ADEQUADO.
		Abril de 2021	Não menciona problemas com Agentes de Registro. Conceito do relatório é ADEQUADO.
AR Digital Certificadora	Agentes de Registro sem vínculos formais na RAIS	Janeiro de 2019	Não menciona problemas com Agentes de Registro. Conceito do relatório é ACEITÁVEL.
		Dezembro de 2019	Não menciona problemas com Agentes de Registro. Conceito do relatório é ADEQUADO.
		Outubro de 2020	Não menciona problemas com Agentes de Registro. Conceito do relatório é ACEITÁVEL.

Fonte: Relatórios de auditoria operacional das empresas citadas, conforme exercícios mencionados.

61. Nesse conjunto de relatórios, constatou-se que apenas alguns resultados das auditorias mencionam não conformidade com o requisito de regularidade fiscal. Diante da situação apresentada, vale destacar que o item 8.1 do DOC-ICP-08 estabelece que a Diretoria de Auditoria, Fiscalização e Normalização da AC Raiz (DAFN/ITI) pode solicitar esclarecimentos aos executantes das auditorias. O item 8.3 determina que, a qualquer tempo, se a DAFN constatar incorreções, omissões ou descumprimento de norma profissional de auditoria nos relatórios entregues, comunicará o fato à entidade que executou a auditoria. Nesse caso, a entidade de auditoria deverá justificar as incorreções no prazo de 15 dias da data do recebimento da notificação. Caso a entidade de auditoria não apresente as justificativas ou estas sejam consideradas insatisfatórias, o Diretor da DAFN poderá aplicar penalidade, em conformidade com o ADE-ICP-08.G.

62. Em manifestação ao relatório preliminar, a Unidade reconhece a necessidade de melhorias no controle anual de auditorias e a avaliação dos seus respectivos resultados. Acrescenta que estão avaliando a melhor maneira de realizar cruzamentos de dados da situação fiscal, de forma a subsidiar e melhorar as ações de auditoria nas entidades da ICP-Brasil.

63. O entendimento que os riscos associados a fragilidades em auditorias operacionais sejam baixos e a ausência de equipe técnica que realize uma análise mais detalhada sobre os itens verificados nos relatórios de auditoria operacional para confirmação dos elementos necessários à manutenção do credenciamento de entidades são, possivelmente, as causas deste achado. Pelo constatado nas análises, o ITI recebe os relatórios de auditoria, atualiza a planilha de controle com os conceitos aplicados nos documentos e apenas instaura procedimento administrativo de apuração nos casos de auditorias com conceitos 4 (inadequado) e 5 (inaceitável).

64. Por consequência, a ausência de rotina de revisão dos pontos tratados em relatório de auditoria operacional, bem como a não realização de controles complementares sobre os requisitos necessários para manutenção das entidades na ICP-Brasil, leva ao desconhecimento de detalhes observados nas auditorias anuais que poderiam servir de elementos para decisões estruturantes na cadeia de certificação, bem como fornecer informações sobre a efetividade dos trabalhos das auditorias independentes.

4. Fragilidades na sistemática de controle dos Planos Anuais de Auditoria Operacional (PLAAO) e dos relatórios de auditorias operacionais.

65. Verificou-se a necessidade de aprimoramento dos controles internos sobre as auditorias operacionais realizadas para manutenção do credenciamento de entidades junto à ICP-Brasil. Esses trabalhos de auditoria devem ocorrer a partir do primeiro ano civil seguinte à data da publicação no DOU do credenciamento do PSCert, conforme determina o DOC-ICP-08.

66. Questionada sobre os controles internos adotados para acompanhar os Planos Anuais de Auditoria Operacional, conforme dispõe o item 5.1 do DOC-ICP-08, a Unidade respondeu da seguinte forma: "Anualmente as entidades AC, ACT, e AR devem realizar auditoria em seus ambientes, por meio de empresas de auditorias credenciadas junto à ICP-Brasil, conforme determina o DOC ICP-Brasil 8. Após a realização de cada auditoria as empresas de auditoria devem fornecer o relatório final ao ITI. O ITI analisa o parecer lavrado nos relatórios e se houver dúvidas na qualidade dos relatórios poderá solicitar os papéis de trabalho. (...) Estando o relatório correto e dependendo do

resultado registrado no parecer do auditor independente a DAFN abrirá processo de fiscalização solicitando explicações da autoridade auditada e determinado a adequação das não conformidades. Se em dois anos consecutivos os relatórios de auditoria apresentar parecer com conceito inaceitável a DAFN abre processo de fiscalização podendo descredenciar a autoridade. Em qualquer situação, poderá o ITI aplicar medida cautelar de suspensão das atividades das autoridades credenciadas durante o processo de fiscalização."

67. A manifestação acima demonstra o processo de análise dos relatórios das empresas de auditoria credenciadas pelo ITI, mas não explicou como é realizado o acompanhamento dos PLAAO que devem ser encaminhados pelas entidades credenciadas até o dia 15 de dezembro de cada ano.

68. Quanto aos controles adotados para acompanhamento dos relatórios de auditorias operacionais executadas por empresas de auditoria independente e órgãos de auditoria interna credenciados junto ao ITI, a Unidade informou que "Atualmente, o ITI não dispõe de sistema de informação para manter os relatórios de auditoria anuais. Ao final de cada ano, as AC enviam o planejamento anual e durante o ano seguinte, realizam auditorias e enviam os relatórios das entidades auditadas. Os relatórios e suas informações são mantidos em planilhas e diretórios específicos. A pedido da CGAFI, está em fase de elaboração um sistema manter as realizações anuais de auditoria das entidades credenciadas junto a ICP-Brasil, porque é entendimento da DAFN que o controle atualmente realizado necessita de melhorias. A CGAFI recebe os relatórios de auditoria, das empresas de auditoria habilitadas, e, por meio do resultado no parecer, a CGAFI realiza acompanhamento e fiscalização com notificação da AR ou AC."

69. Em análise às planilhas mencionadas de acompanhamento dos relatórios de auditoria operacional, verificou-se que não é possível confirmar se todos os Prestadores de Serviço de Certificação (PSCert) estão passando por auditorias anuais para análise dos critérios de manutenção do credenciamento, pois a planilha atualmente adotada para controle apresenta campos com ausência de informações dos relatórios de auditoria entregues, situação confirmada pela não apresentação de alguns relatórios requeridos pela equipe de auditoria através de solicitação de auditoria. Não foram encaminhados à equipe de auditoria nenhum relatório selecionado de ACT, PSBlo, PSC e PSS, bem como relatórios de sete Autoridades de Registro e de uma Autoridade Certificadora. Observou-se também o encaminhamento de relatórios de exercícios diferentes do que foi solicitado pela equipe.

70. Inclusive, o modelo de controle atualmente adotado pela Unidade dificulta o acesso ágil a informações gerenciais sobre os resultados das auditorias, dados que poderiam auxiliar na implementação de medidas estruturantes com impactos positivos para toda a cadeia da ICP-Brasil.

71. Em manifestação por meio do Despacho nº 0489960/2021/CGAFI/DAFN, de 28/5/2021, o ITI apresentou: "De fato, conforme anteriormente informado, o controle dos Planos Anuais de Auditoria Operacional (PLAAO) e dos relatórios de auditorias operacionais é feito de forma manual, pois o ITI não dispõe de sistema de informação para organização dos referidos documentos. Ao final de cada ano, as AC enviam o planejamento anual e durante o ano seguinte, realizam auditorias e enviam os relatórios das entidades auditadas. Os relatórios e suas informações são mantidos em planilhas e diretórios específicos. Quanto à necessidade do sistema, a pedido da CGAFI, está em fase de elaboração um sistema de controle da manutenção das realizações anuais de auditoria das entidades

credenciadas junto à ICP-Brasil, porque é entendimento da DAFN que o controle atualmente realizado necessita de melhorias”.

72. Considerando a fragilidade de controles dos relatórios, verificou-se inclusive situação de ausência de providência tempestiva pelo ITI para acompanhar resultado de relatório de auditoria operacional com conceito inaceitável, em desatendimento ao item 9 do DOC-ICP-08. A AR Águia Corretagem, em 2020, teve o registro de “Conceito Inaceitável” em relatório de auditoria operacional. Questionado sobre as providências para o caso em tela, o ITI informou que o relatório de auditoria operacional da referida AR, emitido em 17 de dezembro de 2020 e entregue ao ITI na mesma data, não contou com instauração de procedimento administrativo de apuração na época devida (Dezembro/2020), apenas em 27/5/2021 foi instaurado o processo SEI nº 00100.001937/2021-15.

73. Conforme define o item 9 do DOC-ICP-08, nos casos de relatórios de auditoria que apresentam conclusão com o Conceito 5 (inaceitável) para as operações do PSCert, cabe à AC Raiz tomar providências cabíveis para garantir a segurança e a confiabilidade da ICP-Brasil, suspendendo inclusive as operações até que as não conformidades apontadas sejam solucionadas. Observa-se, dessa forma, que a ausência de controle adequado sobre as auditorias operacionais prejudica o cumprimento das atribuições estabelecidas na legislação pertinente.

74. Em manifestação ao relatório preliminar de auditoria, a Unidade reconheceu a necessidade de melhorias no controle do planejamento anual de auditorias e a avaliação dos seus respectivos resultados. Informou que já houve no ITI um sistema que fazia esse tipo de controle, mas foi desativado. Por fim, acrescentou que está em elaboração um sistema para controle das auditorias anuais realizadas nos Prestadores de Serviço de Certificação.

75. Diante do exposto, pode-se destacar como possível causa deste achado a avaliação pela gestão do ITI de que os riscos associados às auditorias operacionais realizadas pelas empresas de auditoria independente são baixos, não demandando a priorização de controles complementares para atuar na mitigação dos riscos apresentados nos relatórios, além da deficiência de servidores especializados na CGAFI para realizarem as atribuições regimentais previstas para o setor. A situação culmina em deficiência no acompanhamento das inconformidades registradas, prejudicando a adoção de providências em casos mais relevantes e também de medidas estruturantes para toda a cadeia de certificação.

76. Como consequência, a fragilidade no acompanhamento da manutenção dos critérios de credenciamento acaba permitindo a operação na ICP-Brasil de entidades que não comprovaram a realização de auditorias anuais e que apresentam desconformidades com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

CONTROLES INTERNOS – CADASTRO DE AGENTES DE REGISTRO E CERTIFICADOS EMITIDOS

5. Análise sobre os controles internos implementados para gerenciar o cumprimento dos regulamentos da ICP-Brasil a partir do acompanhamento de dados recebidos das Autoridades Certificadoras.

77. Com o objetivo de avaliar como o ITI gerencia informações relevantes encaminhadas pelas entidades da cadeia de certificação digital para apoiar o aprimoramento constante de controles internos e o alcance dos objetivos da organização, selecionaram-se dados sobre o Cadastro de Agentes de Registro – CAR da ICP-Brasil e também sobre certificados emitidos durante os exercícios de 2020 e 2021. Realizaram-se análises e cruzamentos de dados com as informações recebidas.

78. O Cadastro de Agentes de Registro – CAR é um conjunto formal de dados, gerido pelo ITI, para centralização das informações cadastrais dos Agentes de Registro – AGR que atuam no âmbito da ICP-Brasil. Semanalmente, as ACs ou seus respectivos PSSs encaminham os dados para manutenção do CAR. Apenas os agentes indicados na lista disponibilizada no sítio eletrônico do ITI deverão ter acesso aos sistemas de emissão de certificado digitais, permitindo o controle dos atores que estão habilitados e autorizados a atuar na ICP-Brasil.

79. As informações sobre a emissão de certificados digitais também são encaminhadas pelas Autoridades Certificadoras – AC semanalmente para controle do ITI e contém as características definidas na IN ITI nº 5, de 16 de julho de 2019.

80. As informações estruturadas em arquivos digitais e encaminhadas pelas Autoridades Certificadoras, conforme serão demonstrados nos Achados nº 6 e nº 7, apresentam inconsistências que foram questionadas junto à Unidade, considerando os riscos e a necessidade de averiguação mais detalhada.

81. O resultado dos cruzamentos de dados demonstra que a AC Raiz precisa aprimorar procedimentos estabelecidos de conferências das informações encaminhadas pelas entidades, de modo a manter um ambiente de controle forte, gerenciando riscos e potenciais fraudes. As rotinas de verificação das bases de dados encaminhadas precisam de constante aperfeiçoamento para que se confirme o cumprimento dos normativos regulamentares. Os dados encaminhados são normalmente utilizados para consultas de informações, conforme será adiante apresentado.

6. Fragilidades nas informações divulgadas no Cadastro de Agentes de Registro – CAR.

82. O ITI normatizou o Cadastro de Agentes de Registro – CAR, que constitui um conjunto formal de dados para centralização das informações cadastrais dos Agentes de Registro – AGR que atuam no âmbito da ICP-Brasil. Esses agentes são as pessoas responsáveis por realizar a identificação dos requerentes de certificados, por meio dos atendimentos presenciais, validando a documentação exigida para a emissão de certificados e executando as principais atividades finalísticas das Autoridades de Registro – ARs.

83. Semanalmente, o ITI disponibiliza em seu sítio eletrônico a relação dos Agentes de Registro cadastrados no CAR, conforme informações enviadas pelas Autoridades Certificadoras – ACs. Segundo o art. 5º da IN ITI nº 11, de 23 de outubro de 2020, as ACs deverão manter o acesso em seus sistemas de emissão de certificados digitais somente os Agentes de Registro relacionados na lista disponibilizada no site do ITI, devendo revogar os acessos daqueles Agentes de Registro que deixarem de figurar na relação.

84. Selecionado o Cadastro de Agentes de Registro para análise das informações armazenadas na base de dados utilizada como apoio para confirmação dos atores que podem atuar no âmbito da ICP-Brasil, após utilização da técnica de cruzamento de dados, observou-se o que adiante segue:

a) Não comprovação de vínculo funcional entre 15.477 Agentes de Registro (AGR) e as respectivas Autoridades de Registro (AR) credenciadas junto à ICP-Brasil.

85. O DOC-ICP-03.01, que estabelece as características mínimas de segurança para as ARs, dispõe em seu item 2.1.2 que não são admitidos estagiários nem funcionários terceirizados no exercício das atividades de Agente de Registro. Esses agentes, que realizam a identificação dos requerentes na solicitação de certificados, devem ser funcionários ou servidores da própria organização credenciada como AR junto à ICP-Brasil.

86. De acordo com os cruzamentos de dados efetuados pela equipe de auditoria, do total de 42.412 agentes identificados em planilha encaminhada pelo ITI, mais de 15 mil Agentes de Registro não apresentam vínculo formal na Relação Anual de Informações Sociais - RAIS 2019 ou 2020, conforme alguns exemplos apresentados no quadro a seguir:

Quadro 3 – Agentes de Registro sem vínculos formais na RAIS 2019 ou 2020

Autoridades de Registro	Agentes não localizados na RAIS 2019 ou 2020
NOSSO CERTIFICADO	436
FACILITA CERTIFICADO DIGITAL	387
AR CNDL	320
DIGITAL CERTIFICADORA	280
AR FUTURA	249
AR BRSIGN	220
AR CERT ALPHA	185

Fonte: Cruzamento de dados entre o Cadastro de Agentes de Registro – CAR e RAIS 2020 e 2019.

87. Verificou-se que 22 empresas apresentam mais de 100 agentes não localizados na RAIS. Aprofundando um caso identificado no cruzamento, observou-se empresa em que nenhum dos CPFs dos agentes listados no CAR constam no registro da RAIS de 2019 ou 2020 da empresa, no qual constam somente outros dois diferentes CPFs vinculados.

88. A Unidade apresentou manifestação sobre o achado nos seguintes termos: “De forma geral, entendemos que o cruzamento de dados de vinculação dos AGR com a Autoridade de Registro levando em consideração o vínculo trabalhista, necessita ser aprimorado para refletir melhor a realidade detectada, pois existem exceções nas normas da ICP Brasil que permite o vínculo do AGR a AR, sem a necessidade de vínculo trabalhista, tais como sócios da empresa e funcionários das serventias extrajudiciais. Em relação às constatações de divergências entre os dados da planilha do

Cadastro de Agentes de Registro - CAR fornecida pelo ITI e a correlação com Relação Anual de Informações Sociais - RAIS, verificou-se que há casos em que a AR tem cartórios como entidade vinculada. Como exemplo, cita-se a AR ARPEN (Associação dos Registradores de Pessoas Naturais), a AR CNB CF (Colégio Notarial do Brasil - Conselho Federal). Nesses casos, os Agentes de Registro não possuem vínculos empregatícios com a AR e sim com os cartórios/serventias onde estão lotados. O caso citado que envolve expressivamente uma entidade do setor privado será verificado exclusivamente.”

89. Conforme o DOC-ICP-03.01, que estabelece as características mínimas de segurança para as ARs, procede a afirmação sobre o tratamento especial para os funcionários das serventias extrajudiciais atuarem como Agentes de Registro, sendo tratado no item 2.1.2.1 do normativo. Entretanto, tomando como exemplo a AR ARPEN, citada na manifestação da Unidade, a equipe de auditoria verificou os CPFs vinculados a essa entidade na relação do Cadastro de Agentes de Registro e realizou cruzamento com a RAIS 2019 e 2020. Constatou-se a inexistência de vínculos funcionais da maioria dos CPFs indicados, seja com as associações ou mesmo com os cartórios, conforme se verifica em extrato apresentado no quadro a seguir.

Quadro 4 – Funcionários de serventias extrajudiciais sem vínculos na RAIS 2019 ou 2020

CPF	CNPJ_Empregador	AC	AR	RAIS 2020	RAIS 2019
80336671253	679163000142	AC CERTISIGN	AR ARPEN SP	-	-
36715757860	679163000142	AC CERTISIGN	AR ARPEN SP	-	-
63933462215	679163000142	AC CERTISIGN	AR ARPEN SP	-	-
35647822819	679163000142	AC CERTISIGN	AR ARPEN SP	-	-
57896941600	679163000142	AC CERTISIGN	AR ARPEN SP	-	-

Fonte: Cruzamento de dados entre o Cadastro de Agentes de Registro – CAR e RAIS 2020 e 2019.

90. A situação apresentada demanda análise do ITI, a fim de garantir a conformidade com os requisitos de segurança de pessoal exigidos no DOC-ICP-03.01. Ademais, o cruzamento de dados realizado apresenta diversas Autoridades de Registro que não se enquadram na situação dos cartórios e que também não comprovaram a regularidade da contratação dos Agentes de Registro na forma definida nos normativos da ICP-Brasil.

91. Em manifestação ao relatório preliminar, a Unidade explicou o que seria a AR ARPEN SP e a AR CNBSP, ressaltando que o DOC-ICP-03 permite às serventias extrajudiciais autorizadas pelo Conselho Nacional de Justiça, desde que formalmente vinculadas a uma AR já credenciada, ter seus funcionários habilitados a atuar como agentes de registro. Ressaltou o ITI que não há vínculo empregatício diretamente com a ARPEN e a CNBSP. Informou que o cartório é um associado e a norma permite que os funcionários exerçam a função de Agente de Registro. A Unidade entendeu como equivocada a análise e apontamento de irregularidade nos 1.541 AGRs da AR ARPEN e nos 489 AGRs da CNBSP sem vínculo empregatício. Por fim, mencionou que existe a situação em quem a AR é uma microempresa e o empresário é o AGR, não havendo, neste caso, relação de emprego.

92. Considerando o posicionamento da Unidade e em razão do que dispõe o item 3.2.2 do DOC-ICP-03 sobre as serventias extrajudiciais, esta equipe de auditoria retirou do Quadro 3 o quantitativo inicialmente destacado de AGRs relacionados à AR ARPEN SP e à AR CNBSP. Entretanto, é relevante acompanhar as exigências de habilitação dos funcionários de cartórios como agentes de registro, uma vez que se verificou ausência de vínculos funcionais da maioria dos CPFs indicados no cadastro,

seja com as associações ou mesmo com os cartórios, o que requer avaliação sobre as características de segurança exigidas das entidades, conforme dispositivos do DOC-ICP-03.01.

93. A conferência dos requisitos de segurança de pessoal deve ser analisada no âmbito das auditorias operacionais realizadas nas entidades da ICP-Brasil, a fim de verificar a conformidade com os normativos aplicáveis.

94. A evidenciação de elevado percentual de não cumprimento da regra que impõe a necessidade de vínculo empregatício dos Agentes de Registro gera alerta para a implementação de procedimentos de controle complementares sobre o CAR, antes da ampla divulgação no sítio do ITI das informações cadastrais dos agentes que atuam no âmbito da ICP-Brasil, bem como a cobrança de justificativas junto às empresas que executaram as auditorias operacionais nas entidades a fim de apresentar esclarecimentos sobre este achado.

95. Ademais, como já destacado neste relatório, os apontamentos desta equipe de auditoria precisam de checagem complementar pela Unidade examinada para confirmação de situações específicas sobre as inconsistências apresentadas, a fim de que sejam validados os alertas gerados pelos cruzamentos de dados e a avaliação sobre medidas de controles a serem implementadas. A Unidade poderá trazer medidas adicionais de conferências adotadas no Plano de Ação que deverá apresentar após o recebimento do relatório definitivo.

b) Identificação de 25 Agentes de Registro falecidos, 1 menor de idade, 3 com CPFs não válidos e 4 maiores de 80 anos sem vínculo trabalhista na relação do Cadastro de Agentes de Registro – CAR.

96. O resultado do cruzamento de dados entre as informações do Cadastro de Agentes de Registro - CAR e a situação dos CPFs dos agentes na base da Receita Federal identificou condições como: 25 CPFs de agentes com situação de falecimento, 1 menor de idade (nascido em 2014), 3 com CPFs não válidos e 4 maiores de 80 anos sem vínculo trabalhista.

97. Questionada sobre este achado, a entidade se manifestou da seguinte forma: “A possibilidade de cruzamento de informações para a validação de dados trará mais consistência ao cadastro. Entretanto, as informações fornecidas pelas AC e AR relativas aos Agentes de Registro são de grande valia para as atividades de fiscalização. Anteriormente à instituição do Cadastro de Agentes de Registro (Instrução Normativa 09/2017, de 13/11/2017), o ITI não possuía uma base centralizada com informações dos Agentes de Registro. Em relação aos casos de Agentes de Registro falecidos, as entidades identificadas serão acionadas e intimadas a explicar a não atualização do cadastro. Quanto aos maiores de 80 anos trata-se apenas de uma citação que não oferece risco ao sistema de certificação. Já quanto ao menor de idade é tipicamente erro de cadastro.”

98. As ocorrências constatadas sugerem a necessidade de revisão constante do conjunto de dados enviados pelas Autoridades Certificadoras para composição do CAR, em razão do risco de manutenção de acesso aos sistemas de emissão de certificados digitais a agentes que não apresentam condições de atuação, fornecendo informações desatualizadas aos cidadãos interessados, inclusive com possível abertura para a ocorrência de procedimentos indevidos em descumprimento aos normativos da ICP-Brasil.

99. Quanto aos idosos e ao agente cadastrado com sete anos de idade, apesar da Unidade se posicionar pela inexistência de risco para o sistema de certificação, diante das responsabilidades regulamentares do ITI, é relevante que seja verificada a efetiva atuação desses agentes nos últimos anos, identificando quantos certificados contaram a participação desses agentes, a fim de observar a regularidade dos processos sob seus acompanhamentos ou também a possibilidade de erro no cadastro no CAR.

100. Mesmo a Unidade indicando não haver risco quanto aos agentes que apresentam idade superior a 80 anos, é importante ressaltar que os 4 idosos indicados no levantamento não apresentam vínculo na RAIS 2020, em descumprimento ao DOC-ICP-03.01, que estabelece as características mínimas de segurança para as ARs.

101. Em manifestação ao relatório preliminar, a Unidade reconheceu a necessidade de melhorias no controle de AGRs. Informou que novas regras automatizando a análise dos dados recebidos serão implantadas.

102. A implementação de rotina de controles complementares dos dados disponibilizados pelo ITI em seu sítio eletrônico pode afastar inconsistências nas informações cadastrais dos Agentes de Registro, bem como coibir a participação na emissão de certificados digitais de agentes que não estejam com situação cadastral habilitada para atuar na ICP-Brasil. Conforme informado anteriormente, a atualização do CAR é semanal, entretanto, ainda ocorreram as situações apresentadas neste item.

c) Manutenção de 333 Agentes de Registro na base de dados do CAR com vinculação a Autoridades de Registro (AR) descredenciadas ou indeferidas.

103. Verificou-se a permanência de assentamento no CAR de Agentes de Registro com vinculação a CNPJ de entidades que já estão descredenciadas ou foram indeferidas, conforme quadro a seguir:

Quadro 5 – Quant. de Agentes de Registro vinculados a entidades descredenciadas e indeferidas

Situação	Quant. CNPJ	Quant. de AR	Quant. de CPF
Descredenciado	30	38	208
Indeferido	3	4	125
Total	33	42	333

Fonte: Cadastro de Agentes de Registro (CAR) e Planilha ITI (ACs_e_ARS_info_Auditoria_proc_00100002628_2020_73.xls)

104. O quadro acima demonstra quantidade de Autoridades de Registro (AR) maior que a quantidade de CNPJ, uma vez que se identificou a situação de mais de uma AR estar vinculada a um mesmo CNPJ no cadastro.

105. Conforme o item 4.2.2.4, b, VI, do documento DOC-ICP-03, nas hipóteses de descredenciamento de AR, a AC à qual a AR descredenciada estava operacionalmente vinculada deverá excluir Agentes de Registro do Cadastro de Agentes de Registro - CAR. A não adoção do procedimento possibilita a publicação desatualizada da relação dos agentes no sítio do ITI, prejudicando a confirmação se determinado agente está habilitado e autorizado a atuar no âmbito da ICP-Brasil.

106. Em manifestação, a Unidade afirmou que “será avaliado a implementação de controle para verificar a situação da entidade no sistema CASA, para possibilitar a exclusão automática no CAR (publicado na página do ITI) dos AGR de entidades DESCREDENCIADA, INDEFERIDO ou qualquer outra situação diferente de CREDENCIADO. Adicionalmente, de acordo com as normas do CAR, a AC deve inserir no arquivo semanal os dados dos Agentes de Registro de entidades "em credenciamento", torna-se necessária a inserção de rotina de comunicação à AC para que seja atualizada a base nos casos de indeferimento de credenciamento de AR e para os casos de descredenciamento de AR.”

107. Após a comunicação do relatório preliminar, a Unidade acrescentou que reconhece a necessidade de melhorias no controle dos Agentes de Registro e que já foram implementadas algumas medidas pela CGNPE/DAFN para aprimorar a validação dos dados apresentados pela AC/AR, conforme Ofício Circular nº 3/2021/DAFN-ITI. Afirmou que novas regras automatizando a análise dos dados recebidos serão implantadas.

108. O estabelecimento de controles internos destinados a checar periodicamente dados do Cadastro de Agentes de Registro com informações disponíveis em sistemas governamentais pode contribuir para a publicação de dados mais fidedignos pelo ITI e afastar a atuação indevida de Agentes de Registro inativos, conforme asseguram os normativos da ICP-Brasil.

d) CNPJs de empresas mencionadas no CAR não localizados na base de empresas credenciadas na ICP-Brasil, envolvendo a vinculação de 7.099 Agentes de Registro.

109. Realizados cruzamentos de dados com as informações recebidas do Cadastro de Agentes de Registro - CAR, verificaram-se ocorrências como: registro de "CNPJ de Empregadores" não localizado na base de empresas credenciadas pela ICP-Brasil, bem como registro do mesmo CNPJ para empresas diferentes. A situação encontrada pode ser resumida no quadro a seguir:

Quadro 6 – CNPJs mencionados no CAR não localizados na base de empresas credenciadas

Situação	Qtde CNPJ	Qtde de AR	Qtde de CPF de Agentes de Registro
Não localizados	2449	2663	7099

Fonte: Cadastro de Agentes de Registro (CAR) e Planilha ITI (ACs_e_ARS_info_Auditoria_proc_00100002628_2020_73.xls)

110. O quadro acima demonstra quantidade de Autoridades de Registro (AR) maior que a quantidade de CNPJ, uma vez que ocorre a situação de mais de uma AR estar vinculada a um mesmo CNPJ no cadastro.

111. Sobre o apontamento, a Unidade informou que “em relação ao apontamento "CNPJ de Empregadores" não localizado na base de empresas credenciadas fazemos referência ao item 13.2, a respeito da ARPEN Associação dos Registradores de Pessoas Naturais, ao CNB Colégio Notarial do Brasil cujos funcionários estão vinculados aos CNPJ dos cartórios que estão vinculados a essas AR. Verificou-se, ainda, a existência de vínculos duplicados referentes à AR CNDL (Confederação Nacional de Dirigentes Lojistas) que possuía diversas instalações técnicas secundárias materializada em CNPJ para unidades do SPC Serviço de Proteção ao Crédito em diversos municípios. Possivelmente, após a extinção das Instalações Técnicas - IT e das Instalações Técnicas Secundárias - ITS (Resolução nº 151, de 30/05/2019, do Comitê Gestor da ICP-Brasil), a AR CNDL não atualizou a situação dos Agentes de Registro para "inativo" nos CNPJ desativados. O cruzamento sistematizado

para validação de dados será de grande valia, entretanto, até que se alcance o nível desejado, a alternativa é reforçar a responsabilidade das entidades para a fidedignidade das informações fornecidas ao ITI.”

112. Como apresentado na letra “a” deste item do relatório, ao verificar os CPFs indicados no Cadastro de Agentes de Registro vinculados à AR ARPEN, constatou-se a inexistência de vínculos funcionais na grande maioria dos casos analisados, nem com a própria Associação ou mesmo com algum cartório. O ITI precisa analisar a situação das serventias extrajudiciais, a fim de que o cadastro possa ser atualizado com a chave de CNPJ de entidade credenciada na ICP-Brasil, a fim de permitir os controles adequados.

113. Destacam-se como causas dos itens apresentados neste achado a fragilidade no formato de alimentação da base de dados do Cadastro de Agentes de Registro. Por não ser operado por sistema informatizado, com integração entre bases de dados, não se verifica a confirmação de informações relevantes, além de permitir a inclusão de dados sem observância das exigências normativas. Ao permitir a inserção de CNPJ de empresa que não consta no cadastro das empresas credenciadas ou mesmo de CPF de menor de idade na base, por exemplo, observa-se a demanda por adoção de controles internos complementares, como a rotina de cruzamento de dados, a fim de evitar inconsistências nas informações armazenadas e disponibilizadas posteriormente ao público.

114. Como consequência, além da divulgação de dados no sítio eletrônico do ITI sem o tratamento necessário, o controle frágil do cadastro demonstra a possibilidade de agentes estarem ativos em atividades das ARs sem o cumprimento dos requisitos mínimos de segurança estabelecidos nos normativos da ICP-Brasil, inclusive com acesso a dados pessoais sensíveis e senhas de sistemas de certificação, situação que demanda observação e adoção de medidas pela gestão.

7. Fragilidade nos controles sobre dados de certificados digitais emitidos encaminhados pelas Autoridades Certificadoras.

115. Solicitados os dados de certificados emitidos em 2020 e 2021, realizou-se cruzamento das informações com bases de dados governamentais disponíveis, a fim de confirmar a consistência dos dados disponibilizados pelas Autoridades Certificadoras e os controles implementados pela AC Raiz para acompanhar o cumprimento dos normativos da ICP-Brasil. Diante das análises realizadas detectaram-se inconsistências que serão apresentadas nos itens a seguir.

116. Inicialmente, convém destacar que a equipe também solicitou dados sobre os Agentes de Registro que participaram da emissão de cada certificado. Entretanto, o ITI informou que não tem o registro dessa informação na atual base de dados, sendo necessária solicitação específica para as respectivas Autoridades Certificadoras.

a) Emissão de 11.545 certificados digitais com participação de Autoridade de Registro com inscrição do CNPJ baixada.

117. Em amostras realizadas, identificaram-se registros de certificados emitidos com participação de Autoridades de Registro que apresentam inscrição do CNPJ baixada na Receita Federal. Inicialmente, realizou-se teste numa amostra menor que identificou 201 casos de certificados com

data de emissão posterior à data do registro de baixa da empresa no sistema da Receita Federal. Ao ampliar o teste com dados das empresas identificadas na base de certificados emitidos em 2020 e 2021, verificou-se o total de mais de 11 mil certificados emitidos após a data do registro de baixa das empresas.

118. A Unidade se manifestou sobre este item, explicando que cabe à Autoridade Certificadora implantar sua DPC (Declaração de Práticas de Certificação) e criar meios de forma precisa para realizar a confirmação da identidade de uma pessoa jurídica. Porém, o Comitê Gestor não definiu regras para o ITI auditar e fiscalizar certificados emitidos com CNPJ baixados, mesmo porque os certificados podem ter sido emitidos antes dos CNPJs serem baixados. A revogação do certificado não é automática e deve ser provocada pela pessoa jurídica, por algum outro órgão público e não o ITI.

119. Destacou ainda a Unidade que também deve ser analisado se, após um CNPJ ser baixado, as atividades da empresa ficam extintas e seus efeitos em negócios jurídicos, processos administrativos e judiciais também se encerram. As relações ficariam prejudicadas caso os certificados fossem revogados.

120. Apesar da justificativa de não ter o Comitê Gestor da ICP-Brasil definido regras para o ITI auditar e fiscalizar certificados emitidos com CNPJs baixados, diante do alerta gerado pelos cruzamentos realizados no presente trabalho de auditoria, entende-se que a Unidade pode trabalhar na implementação de medidas para acompanhar a situação das empresas que continuam participando da emissão de certificados digitais sem a manutenção dos critérios exigidos no credenciamento. Além disso, convém que o ITI acompanhe como as auditorias operacionais se posicionaram sobre a regularidade fiscal das empresas nos relatórios anuais, a fim de implementar medidas apropriadas para enfrentar o registro destacado.

121. Em resposta ao relatório preliminar, a Unidade questionou ainda o quantitativo indicado pela equipe de auditoria quanto aos certificados emitidos posteriores à data de baixa na Receita Federal, considerando a planilha que foi encaminhada ao ITI por meio de Solicitação de Auditoria. A Unidade acrescentou que realizou testes nos cinco primeiros casos da lista inicialmente apresentada pela equipe e verificou que tratavam de renovação de certificado. Explicou que a renovação ocorre quando o titular possui um certificado válido e faz uso do mesmo para emitir um novo, sem a participação da Autoridade de Registro no processo de emissão. Portanto, esses casos não se enquadrariam na situação de emissão de certificados digitais com participação de AR com inscrição baixada.

122. Sobre o assunto, esta equipe de auditoria providenciará o encaminhamento à Unidade, juntamente com este relatório definitivo, da planilha que consolida os testes complementares realizados e totaliza o quantitativo apontado neste achado. Vale aqui novamente destacar que os itens apresentados neste relatório demandam procedimentos de checagem complementar pelo ITI para avaliar as situações específicas, a fim de validar o alerta indicado e permitir identificar a necessidade de medidas estruturantes dentro da cadeia de certificação digital. O importante é verificar as situações de inconsistências identificadas, construídas a partir de evidências resultantes dos cruzamentos de bases de dados, para que sejam adotadas medidas de mitigação ou correção da circunstância apresentada.

b) Registro de emissão de 25 certificados digitais para titulares falecidos.

123. Identificaram-se na amostra realizada três casos de titulares de certificado com registro de falecimento na base da Receita Federal e com emissão de certificados do tipo "Pessoa Física" após a data de atualização do óbito, totalizando 25 certificados emitidos na situação.

Quadro 7 – Certificados emitidos para titulares com registro de falecimento

CPF_titular	Descrição_tipo_uso	Data Certificação	Ano Óbito
***531128**	Pessoa Física	Certificado emitido em 29/1/2020	2018
***560018**	Pessoa Física	3 certificados emitidos em 2020 e 13 certificados em 2021	2019
***46898**	Pessoa Física	8 certificados emitidos em 2021	2020

Fonte: Base de dados do ITI sobre certificados emitidos e base de dados da Receita Federal.

124. Ademais, além dos casos referidos, cabe o registro da identificação de 153 titulares ativos de certificado na base 2020 e 2021 com registro de falecimento no cadastro da Receita Federal. Sobre esses casos, 93 titulares foram identificados em amostra aleatória (envolvem 262 certificados emitidos) e os outros 60 casos foram identificados a partir de uma segunda amostra envolvendo 20.000 CPFs (envolvem 75 certificados emitidos).

125. Importa destacar que o último teste realizado considerou o universo de 5.916.890 titulares, selecionando uma amostra de 20.000 CPFs. Como a base de certificados ativos é bem superior aos registros analisados pela equipe, infere-se haver ainda mais registros de falecimento entre os certificados ativos.

126. Em manifestação, a Unidade informou que não há como realizar emissão de certificado digital presencial para pessoas falecidas, exceto em caso de fraude. A forma presencial exige identificação documental e biométrica. Pode o ocorrer o falecimento do titular após a emissão do certificado digital. Também pode ocorrer a renovação do certificado conforme registrado nas DPCs das Autoridades Certificadoras e aqui transcrito:

3.3.2 Esse processo será conduzido segundo uma das seguintes possibilidades: a) adoção dos mesmos requisitos e procedimentos exigidos nos itens 3.2.2 e 3.2.3; b) **solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado ICPBrasil válido, do tipo A3 ou superior**, que seja do mesmo nível de segurança ou superior, limitada a 1 (uma) ocorrência sucessiva, quando não tiverem sido colhidos os dados biométricos do titular, permitida tal hipótese apenas para os certificados digitais de pessoa física. Na hipótese de o certificado utilizado para a identificação não ser emitido pela AC SOLUTI MULTIPLA, o solicitante declarará, sob pena de revogação do certificado, que se trata de primeira renovação.

127. Ressaltou que qualquer titular que já tenha um certificado digital com os dados biométricos colhidos pode solicitar a renovação uma vez por igual período. Um Certificado (A3) tem três anos de validade, sem a necessidade de ir a uma Autoridade de Registro para ser renovado. A renovação é eletrônica por meio do certificado válido que está para expirar seu prazo de validade. Destacou que muitos certificados são emitidos para serem usados em negócios com empresa individual onde o filho, esposa ou irmão podem manter o certificado para não parar o negócio jurídico.

128. O ITI destacou que não dispõe de mecanismo para detectar se o titular de um certificado faleceu e se seu certificado ainda está em uso. Informou que com grande dificuldade conseguiu uma base de dados com relação de possíveis falecidos. Feitas pesquisas e contatos com endereço dos titulares, foram evidenciados registros com o falecimento. O ITI determinou a revogação de vários certificados junto às ACs. As Autoridades Certificadoras informaram que não tinham mecanismos para fazer a prova de vida dos titulares. O resultado desse trabalho em 2015 foi alguns certificados digitais revogados e outro não por ordem judicial.

129. Fundamentou que o trabalho realizado da prova de vida do titular não é de competência do ITI nem da Autoridade Certificadora. Ao ITI cabe apenas fiscalizar se os procedimentos de identificação da pessoa solicitante estão sendo realizados conforme as Normas da ICP-Brasil no momento da solicitação. Ressaltou que não verifica como essa auditoria possa associar algum tipo de falha de controle ao processo de emissão de certificado digital relativa a titulares de certificados que faleceram após a emissão do certificado.

130. Apesar do relato dos gestores, convém salientar que os casos evidenciados no Quadro 7 são de certificados emitidos após o falecimento do titular, conforme cruzamento de dados registrados na base da Receita Federal. Como responsável por auditar e fiscalizar as entidades da ICP-Brasil, o ITI tem competência para solicitar esclarecimentos das Autoridades Certificadoras que participaram da emissão dos referidos certificados, a fim de conferir o processo, confirmar as informações e tomar as providências devidas.

131. Em manifestação ao relatório preliminar, a Unidade reforça os esclarecimentos já prestados e informa que será necessária apuração individualizada por parte da AC. Acrescenta que está nos ajustes finais para o acesso à base de dados do CPF mantida pela Receita Federal, o que poderá permitir a adoção de rotina para verificação da situação detectada pela equipe de auditoria.

132. O ITI destacou que todos os 25 certificados emitidos foram na modalidade de “certificado digital”, que significa reemissão utilizando certificado digital válido possivelmente emitido antes do óbito. Nessa situação, não haveria desconformidade da AC ou AR, pois não é possível aos entes da ICP-Brasil realizar o batimento com a base de óbitos.

133. Conforme informado pela Unidade, os casos constatados ocorreram em situação de renovação do certificado, o que requer análise sobre medidas de controle para situações como as identificadas neste item. Salienta-se a necessidade de acordo entre o ITI e a Secretaria Especial da Receita Federal do Brasil para compartilhamento de dados, de modo a permitir a verificação da ocorrência de casos de falecimento, impedir a emissão de novas certificações utilizando os dados de pessoa falecida, bem como providenciar as medidas de cancelamento dos certificados vigentes.

c) Certificados emitidos que apresentam nomes de titulares diferentes para um mesmo CPF.

134. Verificaram-se casos de certificados emitidos com registro de nomes de titulares divergentes para um mesmo CPF. Como destaque, menciona-se a situação de certificados emitidos do tipo "Pessoa Física" para um mesmo CPF, mas com um titular registrado em nome feminino e outro em nome masculino, conforme exemplos do quadro a seguir:

Quadro 8 – Exemplos de certificados emitidos para o mesmo CPF com nome do titular diferente

Ano	CPF_titular	Data_da_certificação
2021	**61932**	27/04/2021 16:45:00
2021	**61932**	27/04/2021 16:41:00
Ano	CPF_titular	Data_da_certificação
2020	**26130**	06/01/2020 10:09:34
2021	**26130**	11/03/2021 09:39:52
2020	***569978**	07/07/2020 21:33:32
2020	***569978**	05/06/2020 22:33:02
2020	***569978**	30/07/2020 23:03:05

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021. (*) As iniciais dos nomes dos titulares foram suprimidas no relatório definitivo.

135. Observaram-se situações também de registro de certificados do tipo "Pessoa Jurídica", com o cadastro de um mesmo CPF, mas com nomes de titulares responsáveis diferentes, conforme exemplos a seguir.

Quadro 9 – Exemplos de certificados emitidos do tipo “Pessoa Jurídica” com o mesmo CPF cadastrado para titulares diferentes

Ano	CPF_titular	Data_da_certificação
2020	**73068**	22/01/2020 13:00:00
2020	**73068**	11/02/2020 13:00:00

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021. (*) As iniciais dos nomes dos titulares foram suprimidas no relatório definitivo.

136. Ainda, identificaram-se certificados do tipo "Pessoa Física", com o campo "Nome_titular" registrado para uma pessoa jurídica, conforme exemplos do quadro a seguir.

Quadro 10 – Certificados emitidos do tipo “Pessoa Física” com o titular registrado para pessoa jurídica

Ano	CPF_titular	Nome_titular
2020	***087868**	F e A Clinica Medica e Odontologica LTDA
2020	***243393**	B Engenharia LTDA

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021.

137. Importa mencionar que o DOC-ICP-05 determina como obrigatório o preenchimento do nome completo, sem abreviações, no campo específico do certificado de uma pessoa física, conforme informações constantes nos documentos apresentados (Item 3.2.3.2.1). No caso de certificados de uma pessoa jurídica, é obrigatório o preenchimento do nome completo do responsável pelo certificado, sem abreviações (Item 3.2.2.3.1).

138. Em manifestação, a Unidade informou que cada caso merece análise específica. Pode haver erro na emissão de certificados, que devem ser revogados pelas ACs. Pode haver certificados com pessoas que alteraram seus nomes, como pode ocorrer erro na geração dos arquivos que são informados ao ITI. Ressaltou que a base não é do ITI, mas sim das ACs. O ITI solicita cópia das informações para poder realizar auditorias e fiscalizações e encontrar irregularidades na emissão.

139. Após o recebimento do relatório preliminar, o ITI manteve os esclarecimentos já prestados e destacou a necessidade de apuração individualizada por parte da AC. Informou que está em ajustes finais para acesso à base do CPF mantida pela RFB e será possível posteriormente adotar uma rotina

de verificação. Acrescentou que a base de certificado deve refletir tão somente os dados recebidos das AC, reafirmando não haver erro no cadastro.

140. Considerando as manifestações da Unidade, diante da responsabilidade por realizar auditorias e fiscalizações, identificando possíveis irregularidades na emissão dos certificados, convém que os casos apresentados nos resultados dos cruzamentos sejam analisados para que as exigências dos normativos da ICP-Brasil sejam cumpridas, principalmente quanto à correta identificação do responsável pelo certificado, que é a base da segurança da certificação digital. Ademais, medidas de controle também precisam ser revistas para avaliar a ocorrência de erros de cadastro e proporcionar proteção razoável às operações.

d) Ausência de informações sobre as Autoridades de Registro (AR) responsáveis pelo encaminhamento de solicitações de emissão de certificados em mais de 50 mil registros.

141. Constatou-se o não preenchimento das colunas CNPJ_AR e Nome_AR em 51.201 registros de certificados emitidos no período de 2020 e 2021. Conforme DOC-ICP-05, a submissão da solicitação de certificado deve ser sempre por intermédio da AR. Ademais, o DOC-ICP-04, no item 7.1.4.1, prevê a inclusão do CNPJ da Autoridade de Registro no certificado digital.

142. A situação identificada envolve 38 Autoridades Certificadoras, com o registro de 47.965 CPFs, sendo os casos mais recorrentes a seguir demonstrados:

Quadro 11 – Certificados emitidos sem informações sobre as Autoridades de Registro (AR)

Autoridade Certificadora	Quantidade CPF_titular	Percentual
AC OAB G3	18955	37%
AC CERTISIGN RFB G5	6997	14%
AC SOLUTI MULTIPLA V5	6069	12%
AUTORIDADE CERTIFICADORA SERPRORFBV5	5780	11%
AC VALID RFB V5	2491	5%
AC SOLUTI-JUS V5	2038	4%
AC SERASA RFB V5	1912	4%
AC IMPRENSA OFICIAL SP RFB G5	1574	3%
AC CERTISIGN-JUS G6	900	2%
AC PRODEMGE RFB	861	2%

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021.

143. Em manifestação, a Unidade informou que a Resolução nº 150, de 7 de novembro de 2018, determinou a inclusão do CNPJ da AR. O artigo 3º da mesma resolução determinou um prazo de 120 dias para adequação dos sistemas das ACs. Portanto, foi a partir de abril de 2019 que se tornou obrigatória a inclusão do CNPJ nos certificados. Algumas ACs não cumpriram o prazo, houve atraso na emissão de alguns certificados sem o CNPJ da AR. Destacou que, atualmente, nos certificados emitidos, consta o CNPJ da AR.

144. Considerando a manifestação da Unidade, convém ressaltar que mesmo diante da exigência normativa, certificados foram emitidos, em 2020 e 2021, sem a inclusão do CNPJ da AR onde ocorreu a identificação presencial. A ausência dessa informação, além de descumprir exigência da ICP-Brasil, prejudica possível rastreio de dados sobre o certificado, o que demanda atuação do ITI para cobrança da correta disponibilização dos identificadores exigidos.

145. Em esclarecimentos encaminhados após o relatório preliminar, a Unidade destacou que a ausência do nº do CNPJ pode representar uma não conformidade no certificado digital, entretanto, informou que já existe rotina implementada na CGAFI para avaliar esse requisito. Registrou que, nas rotinas de importação de certificado, executa-se uma etapa de avaliação de conformidade que verifica diversos itens com o objetivo de manter a padronização dos certificados ICP-Brasil e sempre que ocorre a ausência do CNPJ no local exigido, as ACs são comunicadas para correção futura em seus procedimentos de emissão de certificado, sem revogação do certificado.

146. Do total apresentado pela equipe de auditoria, o ITI analisou por amostragem os dados e acrescentou as seguintes considerações: 845 certificados não se aplicam, pois são do tipo SSL e TS para uso em equipamento e aplicações, com restrições técnicas para o uso; 12 registros testados correspondem à renovação eletrônica, não sendo aplicável o CNPJ da AR. Destaca que o cruzamento de dados da equipe de auditoria pode não ter considerado o tipo de emissão “Certificado digital” ou “Renovação eletrônica”.

147. Diante da última manifestação da Unidade, é importante destacar que os cruzamentos realizados sobre dados de certificados digitais emitidos em 2020 e 2021 foram realizados com base nas informações fornecidas à equipe de auditoria. É preciso que a Unidade examine os demais resultados apresentados para considerar eventuais inconsistências e casos específicos que não se aplicam à questão apontada. Conforme consta no tópico “Recomendações” deste relatório, o ITI deverá adotar providências para verificar as inconformidades, validar os dados dos alertas e aplicar as medidas cabíveis para os casos de irregularidades confirmadas.

e) Certificados emitidos com atuação de Autoridades de Registro (AR) que apresentam inconsistências no assentamento dos vínculos empregatícios de Agentes de Registro.

148. Por meio de cruzamentos realizados entre a base de certificados emitidos (2020 e 2021), a base RAIS (AR com vínculos empregatícios registrados) e a base de dados de Agentes de Registro encaminhada pelo ITI, verificaram-se as seguintes situações, conforme alguns exemplos a seguir destacados:

- i. 130.934 certificados emitidos com participação de 264 Autoridades de Registro cujo CNPJ não apresenta vínculos empregatícios na RAIS:

Quadro 12 – Certificados emitidos com participação de AR cujo CNPJ não apresenta vínculos empregatícios na RAIS

Nome AR	CNPJ	Quant. Certificados emitidos	Quant. Vínculos RAIS	Quant. AGR – CAR
AR BEST WORLD	1382562000100	1642	0	2
AR IAORAMA	3726919000236	15.409	0	21
AR TOP SAFE	23717422000188	15.038	0	16

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021, RAIS e CAR.

- ii. 170.932 certificados emitidos com participação de 169 Autoridades de Registro com registro de menos de 2 vínculos empregatícios na RAIS, mas com quantitativo maior de Agentes de Registro no CAR:

Quadro 13 – Certificados emitidos com participação de AR com indicação de menos de 2 vínculos empregatícios na RAIS, mas com quantitativo maior de Agentes de Registro no CAR

Nome AR	CNPJ	Quant. Certificados emitidos	Quant. Vínculos RAIS	Quant. AGR – CAR
AR TARC	8708557000193	446	1	35
AR CELEBRAR	22106571000148	3060	2	11
AR ONLINE NORDESTE	38016084000124	13634	1	40

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021, RAIS e CAR.

- iii. Certificados emitidos com participação de AR sem agentes de registros localizados no Cadastro de Agentes de Registro – CAR:

Quadro 14 – Certificados emitidos com participação de AR sem Agentes de Registro localizados no Cadastro de Agentes de Registro – CAR

Nome AR	CNPJ	Quant. Certificados emitidos	Quant. Vínculos RAIS	Quant. AGR – CAR
AR QUALITY BETIM CERTIFICACAO	36431513000102	649	0	Não localizado na base de agentes
AR DIGITALLSIGN CERTIFICADORA DIGITAL CWB EIRELI	15003266000165	514	0	Não localizado na base de agentes

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021, RAIS e CAR.

149. Em manifestação, a Unidade destacou que as regras para credenciamento de uma Autoridade de Registro estão definidas no item 7 do DOC-ICP-02 (Política de Segurança da ICP-Brasil), e subitem 2.2.3 do DOC-ICP-03 e seu Anexo II. Configura pré-requisito para o credenciamento a apresentação do relatório de auditoria pré-operacional, momento em que é verificado o vínculo empregatício do AGR. As auditorias pré-operacionais nas Autoridades de Registro são realizadas por empresas credenciadas para esta atividade.

150. Informou ainda que, anualmente, toda autoridade credenciada à ICP-Brasil deve realizar auditoria operacional, momento em que deve ser verificada a habilitação do AGR. A CGAFI entende que tal controle existe, porém pode ser melhorado. Este ano, o ITI assinou contrato com empresa para desenvolvimento de software, objetivando automatizar e criar ferramentas para melhorar os processos de credenciamento, auditoria e fiscalização.

151. Diante da situação identificada, existem Autoridades de Registro atuando sem cumprimento dos requisitos normativos da ICP-Brasil. Conforme apresentou a Unidade, auditorias pré-operacionais e operacionais são realizadas nas entidades, entretanto, o resultado dos cruzamentos revela a necessidade de implementação de medidas de controle complementares para acompanhar o atendimento dos critérios exigidos pela ICP-Brasil pelas entidades credenciadas. Também se mostra necessário conferir os trabalhos de auditorias realizados nas empresas indicadas no cruzamento, a fim de cobrar esclarecimentos aos executantes das auditorias quanto ao requisito de segurança de pessoal.

f) Certificados emitidos com data futura.

152. Verificou-se o registro de 262 certificados emitidos com data futura, envolvendo 239 CPFs e 6 Autoridades de Registro. Importa destacar que a base de dados dos certificados emitidos em 2020 e 2021 foi disponibilizada à equipe de auditoria no dia 7 de junho de 2021. Realizadas as análises dos dados, constataram-se certificados com registro de emissão em data futura, incluindo junho a dezembro de 2021, conforme exemplos apresentados no quadro a seguir.

Quadro 15 – Exemplos de certificados emitidos com data futura

Descrição tipo_uso	CPF_titular	Data_da_certificacao	Data_validade	Nome_AR	Nome_AC
PESSOA FISICA	**87718**	10/07/2021 14:00:44	10/07/2024 14:00:44	AR CNDL	AC CNDL RFB V3
PESSOA JURIDICA	***236501**	27/08/2021 14:05:36	27/08/2024 14:05:36	AR LINK	AC LINK RFB V2
PESSOA FISICA	**48630**	29/09/2021 12:40:42	29/09/2022 12:40:42	AR SAFEWEB	AC SAFEWEB RFB V5
PESSOA FISICA	***823198**	06/12/2021 10:00:00	06/12/2024 10:00:00	AR CNDL	AC CNDL RFB V3

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021. (*) As iniciais dos nomes dos titulares foram suprimidas no relatório definitivo.

153. A situação verificada também pode ser analisada a partir dos dados do quadro a seguir.

Quadro 16 – Números de certificados emitidos com data futura (junho a dezembro de 2021)

CNPJ_AR	NOME_AR	06/2021	07/2021	08/2021	09/2021	10/2021	11/2021	12/2021	Total
01579286000174	AR SAFEWEB	98	22	2	3	2			127
11508222000136	AR LINK	66	10	4	2	4	3		89
14842663000168	AR DOCCLOUD	4	6						10
31725974000166	AR REDE GAUCHA	7	2						9
34173682000318	AR CNDL	14	7	2				2	25
91110262000164	AR SINDILOJAS DE FARROUPILHA	2							2
Total		191	47	8	5	6	3	2	262

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021 (Considerados dados a partir de 8/6/2021).

154. Em manifestação ao relatório preliminar, o ITI destacou que a emissão de certificado com data futura tem previsão normativa e não oferece risco à credibilidade ou segurança do processo de certificação digital. Os certificados com data futura têm o seu uso impossibilitado por qualquer aplicação, considerando a existência dos campos “Not after” e “Not before”.

155. Apesar da Unidade não considerar o apontamento como desconformidade, mantém-se o registro da situação encontrada para que seja atendida recomendação de apresentar os valores que indicam as diferenças de datas referentes à emissão do certificado e ao período que podem efetivamente ser utilizados (“Not after” e “Not before”).

g) Outras situações identificadas na base de dados de certificados emitidos.

156. Verificaram-se ainda as seguintes situações na base de dados de certificados emitidos em 2020 e 2021:

- i. Registros de nº de CNPJ no campo “CPF_titular”;
- ii. Ausência dos nomes de titulares de certificado, divergindo dos requisitos do DOC-ICP-05, que solicita nome completo sem abreviações;
- iii. Grafias diferentes para os nomes de titulares de certificado, inclusive com sobrenomes distintos para o mesmo indivíduo;
- iv. Inserção de números, datas, letras soltas ou apenas prenome no campo “Nome_titular”, divergindo dos requisitos do DOC-ICP-05, que solicita nome completo sem abreviações.

157. Em manifestação, a Unidade destacou o que adiante segue: “a base de dados de certificados no ITI deve espelhar exatamente o que aconteceu na emissão do certificado. Isto não é fragilidade na base. Pode ocorrer erros na emissão de um certificado, fato que obriga a revogação deste pela AC. Há casos em que AC emite um certificado para teste com ausência de parâmetros necessários e o ITI questiona. A AC responde dizendo era teste e que o certificado foi revogado no momento da emissão. O ITI não tem controle de como a AC mantém sua base. A AC deve enviar sua base de acordo como ela está. Tal condição é situação necessária para possibilidade de pesquisa e identificação de irregularidades na emissão de certificados”.

158. Complementou ainda nos seguintes termos: “A prova que a base está atendendo a seu objetivo é o questionamento foi (sic) a pesquisa realizada por essa equipe de auditoria e os questionamentos feitos aqui. A base é utilizada para pesquisa de certificados fraudados e certificados com parâmetros irregulares. Observou corretamente essa equipe de auditoria, com base no DOC-ICP-05, erro no campo nome que não pode ser abreviado. Esse foi o motivo de solicitar a base de certificados e criar um repositório desta aqui no ITI. Por isso, o ITI está em processo de análise e desenvolvimento ferramentas eletrônicas para melhor análise dessas informações.”

159. Também consta nos esclarecimentos da Unidade que as regras para emissão de certificado digital estão definidas no DOC-ICP-05. Nesse documento, estão relacionados os requisitos mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil que devem ser implantados pelas autoridades certificadoras. Cada autoridade implanta sua política denominada ‘DPC’ e informa ao ITI. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços. É neste documento que se define as regras de controle para emissão de um certificado.

160. Acrescentou ainda a Unidade examinada que as funções de auditoria e fiscalização do ITI, com competência limitada e exclusiva no âmbito da ICP-Brasil, deve obediência às regras impostas no escopo determinado pelo Comitê Gestor/ICP-Brasil. O repositório de dados com informações de certificados emitidos é uma ferramenta que foi implantada para ajudar na análise das atividades de Auditoria e de Fiscalização do ITI. Destacou, por fim, que não existe erro na base visto espelhar exatamente o que contém cada certificado emitido por Autoridades Certificadoras.

161. Ressalta-se que a sistemática de envio semanal de dados dos certificados pelas Autoridade Certificadoras ao ITI necessita de aprimoramentos. Na atual sistemática, os dados são transferidos ao ITI por protocolo de transferência de arquivos – FTP e posteriormente, recebidos, conferidos e carregados no sistema SGC2 por servidores do ITI. Caso uma AC não envie os arquivos ou o faça de maneira incorreta, o colaborador responsável entra em contato e solicita o reenvio com a correção. Os dados enviados servem de base para auditorias e fiscalizações, respostas a pedidos de informações da Polícia Federal, análise de fraudes, etc. Para efetuar pesquisas na base de dados é necessária a programação de consultas “queries”, demandando conhecimento especializado do usuário. O processo pode ser automatizado para minimizar o risco de erro e retrabalho, bem como permitindo a adoção de instrumentos de verificação automática e emissão de alertas, relatórios e informações gerenciais, de modo a facilitar o trabalho de fiscalização da DAFN.

162. Destacou, por fim, que o ITI está treinando uma equipe de TI para criar ferramentas eletrônicas com objetivo de auxiliar as atividades de auditoria e fiscalização. Também foi contratada fábrica de software para desenvolvimento e reestruturação do Sistema CASA, responsável por manter o cadastro de autoridades junto à ICP-Brasil. Afirmou que as normas da ICP-Brasil sofreram muitas mudanças e o sistema está defasado, necessitando aprimoramento.

163. Em manifestação ao relatório preliminar, a Unidade manteve os esclarecimentos já prestados e reafirmou que não há fragilidade na base de dados. Destacou que a base de certificados tem o objetivo de espelhar fielmente os dados encaminhados pela AC.

164. Diante de todos os itens apresentados, pode-se destacar como causa deste achado o sistema eletrônico estruturado para registro dos certificados emitidos não possuir integração com outras bases de dados, de forma a permitir a geração de alertas para cadastros inconsistentes e impedir a continuidade do processo de emissão diante da constatação de inconformidades. Ademais, destaca-se a necessidade de aprimorar as rotinas implementadas pelo ITI para controle dos dados encaminhados pelas Autoridades Certificadoras, de forma a confirmar o atendimento das normas da ICP-Brasil.

165. Como consequência, pode-se destacar que a fragilidade nos mecanismos de controle sobre os dados encaminhados a respeito de certificados emitidos favorece à manutenção de certificados operantes que não cumprem os padrões dos normativos da ICP-Brasil, o que demanda esclarecimento dos casos que apontam para possíveis inconformidades ou fraudes.

166. Outra fragilidade que se entende relevante salientar é a ausência de controle no âmbito do ITI sobre as informações dos Agentes de Registro que participam de cada emissão de certificado. Compreende-se que o ITI, pelas suas competências regimentais, precisa dispor dos dados necessários para rastrear qualquer certificado emitido e efetuar as verificações necessárias. A inclusão desses dados na base fornecida pelas Autoridades Certificadoras merece ser analisada no âmbito da Unidade, com posterior encaminhamento da proposta ao Comitê Gestor, caso necessária aprovação.

8. Informação sobre ocorrências identificadas na base de dados de certificados digitais emitidos

167. Diante das manifestações da Unidade que indicaram não haver desconformidade com critérios normativos preestabelecidos, mantém-se o registro dos itens adiante destacados no relatório como informação, sem vinculá-los às recomendações dispostas ao final do trabalho.

a) Multiplicidade de certificados emitidos para um mesmo CPF.

168. Verificaram-se casos de repetições de certificados emitidos para um mesmo titular, na base de dados de 2020 e 2021, em quantidades relevantes que geraram alertas para confirmação da Unidade examinada, conforme se observa no quadro a seguir.

Quadro 17 – Registros de CPFs repetidos na base de dados de certificados emitidos

Quant. De repetições por CPF	Quant. De CPFs envolvidos	Quant. De certificados emitidos
> 10	8840	214968
10	2441	24410
9	3384	30456
8	5404	43232
7	9393	65751
6	18593	111558
5	40106	200530
4	111248	444992
3	327775	983325
2	1287250	2574500

Fonte: Base de dados do ITI sobre certificados emitidos – 2020 e 2021.

169. Como exemplo, pode-se destacar o quantitativo de 46.821 certificados em nome da Secretaria da Fazenda do Ceará, bem como outros casos com resultados de mais de 200 certificados para um mesmo CPF.

Quadro 18 – CPFs com maiores repetições de certificados emitidos na base de dados 2020 e 2021

CPF	Quantidade
05080	734
***272451**	557
***20728**	402
***61158**	339
***532996**	253

Fonte: Planilha “Maiores Repetições” – Elaboração da equipe de auditoria.

170. Por exemplo, na situação do CPF ***152.620-**, somam-se 79 certificados emitidos do tipo Pessoa Física, 93 do tipo Pessoa Jurídica e 1 de Equipamento/Aplicação apenas no período de 2020 e 2021.

171. Somando as maiores repetições, observaram-se 8840 casos de titulares que apresentam mais de 10 certificados emitidos apenas na base de 2020 e 2021.

172. Em manifestação sobre o item, a Unidade informou que o DOC-ICP-04 (Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil) e o DOC-ICP-05 (Requisitos Mínimos para as

Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil) não limitam a quantidade de certificados por pessoa física ou jurídica, ou seja, não existe regra determinando quantos e quais tipos de certificados cada pessoa física ou jurídica pode ter.

173. Como exemplo, destacou a Unidade que um advogado pode ter em seu escritório cinco máquinas, cada uma com um auxiliar de escritório peticionando, e cada máquina com um certificado do tipo A1 do advogado. Uma pessoa jurídica pode adquirir certificados para várias áreas como: RH, Financeira, Contabilidade, Comercial, etc. Cada área com um certificado da pessoa física. Um servidor público pode adquirir vários certificados porque é responsável por várias máquinas (servidores). Também há certificados específicos para instalação em máquinas para validar transações ali realizadas como servidores e máquinas registradoras.

174. Quanto ao caso da Secretaria de Fazenda do Ceará, destacou o ITI que a Sefaz/CE estava implantando o Módulo Fiscal Eletrônico – MFE. Os equipamentos do Módulo Fiscal Eletrônico utilizam certificado ICP-Brasil e registram, de forma eletrônica, as operações comerciais dos contribuintes varejistas do Estado do Ceará. O MFE gera e autentica Cupons Fiscais Eletrônicos – CFE e os transmite, automática e periodicamente, via internet, à Secretaria da Fazenda do Estado do Ceará.

175. Ao final, ressaltou que não cabe ao ITI controlar quando e como o titular utilizará seu certificado digital, assim como a quantidade de certificados digitais que a pessoa física ou jurídica vai adquirir, entendendo o questionamento levantado como irrelevante.

176. Em manifestação ao relatório preliminar, a Unidade reafirma que não há necessidade de estabelecimento de rotina para avaliar a quantidade de certificados emitidos por usuário e que a decisão de adquirir um ou mais certificados é exclusiva do usuário que compra e paga pela aquisição.

177. Diante dos esclarecimentos da Unidade que destaca não caber ao ITI limitar o quantitativo de certificados digitais que as pessoas físicas ou jurídicas estão utilizando, e que a situação não sinaliza riscos para as operações, mantém-se o registro como observação no relatório.

b) Ausência do número de CPF do titular em 18 certificados emitidos.

178. Constataram-se 18 registros de certificados emitidos com o campo “CPF_titular” zerado.

179. Em manifestação, a Unidade destacou as regras definidas no DOC-ICP-04, que destaca a possibilidade de quando números de CPF, NIS, (PIS, PASEP ou CI), RG, CNPJ, CEI ou Título de Eleitor não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres “zero”. A presença de zeros não pode, dessa forma, ser caracterizada como irregularidade, sendo permitida pela norma ICP-Brasil.

180. Conforme informações adicionais apresentadas após o relatório preliminar, o ITI reafirma que não há necessidade de incluir obrigatoriamente o CPF no certificado digital. Destaca que, de acordo com o item 3.2.3.2.1 do DOC-ICP-05, é obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física: nome completo, sem abreviações, e a data de nascimento.

181. Em análise à manifestação da Unidade, importa complementar que o item 3.2.3.2.2 do DOC-ICP-05 destaca que cada Política de Certificado pode definir como obrigatório o preenchimento de outros campos, ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes em documentos, como o caso do Cadastro de Pessoa Física (CPF). Dessa forma, em algumas situações, o preenchimento do campo pode ser obrigatório.

182. Ademais, convém abordar que os termos do normativo DOC-ICP-04 foram editados inicialmente em 2001 e, atualmente, o uso dos dados de CPF foi bastante ampliado, sendo utilizado por diversos sistemas e aplicativos como chave fundamental para o cruzamento de informações. Também não ficou demonstrado nos casos indicados neste item se outro documento foi exigido para identificar o titular do certificado, de forma a atender os campos obrigatórios para os certificados, conforme definição do DOC-ICP-04.

183. Dessa forma, fica o registro como observação da situação encontrada para que a condição de exigência do CPF seja verificada na emissão de certificados digitais, de forma a facilitar o cruzamento de informações, bem como prover maior segurança e confiança nas transações digitais.

c) Emissão de certificados para titulares maiores de 90 anos.

184. Identificaram-se casos de idosos maiores de 90 anos, que tiveram repetidos certificados emitidos na base de dados de 2020 e 2021. Verificou-se que os casos com mais de 6 repetições envolvem 69 CPFs e 794 certificados emitidos. Segue quadro apenas com alguns exemplos, a fim de que o ITI avalie potenciais riscos relacionados às emissões realizadas.

Quadro 19 – Certificados emitidos para idosos maiores de 90 anos

CPF	Nascimento	Idade	Repetição de emissão
08596	05/05/1923	98	35 certificados
25238	22/11/1922	98	7 certificados
09102	18/04/1921	100	8 certificados
09668	22/11/1929	91	75 certificados
019718	04/08/1930	90	52 certificados

Fonte: Base de dados do ITI sobre certificados emitidos em 2020 e 2021 e Base de dados da Receita Federal.

185. Em manifestação, a Unidade informou que não existe regra proibitiva limitando emissão de certificados digitais por motivo de idade. Tal limite, se existisse, deveria ser imposto por lei, Código Civil, o que seria questionável, porque existem pessoas com mais de 90 anos plenamente capazes de exercer seus direitos e deveres sem necessidade de curatela. Entendeu como improcedente o questionamento. Acrescentou que as regras da ICP-Brasil atentam para o controle na emissão do certificado. Deve a Autoridade Certificadora verificar se é procedente a identificação do solicitante no momento da emissão. Mencionou que a competência do ITI não abrange verificação de idade, prova de vida, etc.

186. Apesar do posicionamento da Unidade, esta equipe considera relevante manter o registro da situação como informação, em razão da constante necessidade de revisão dos critérios para identificação dos solicitantes para a emissão dos certificados. Além da idade avançada para utilização de certificados digitais, a repetição de emissões no período compreendido apenas entre os anos de 2020 e 2021 também gera alerta para confirmação da regularidade das operações.

TRANSPARÊNCIA E LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

9. Falhas na divulgação de informações de interesse público no sítio eletrônico do ITI.

187. Consultando informações divulgadas no site da Unidade e considerando questionamentos encaminhados durante o trabalho da auditoria, verificaram-se falhas na divulgação de informações no sítio eletrônico do ITI que necessitaram de ações corretivas para nova publicação.

188. Em análise às auditorias operacionais, verificou-se, por exemplo, que a empresa Crowe Horwath Macro GRC E Tecnologia Ltda estava realizando auditorias nas entidades da ICP-Brasil, sem constar na lista publicada no site do ITI (<https://www.gov.br/iti/pt-br/assuntos/auditoria-e-normalizacao>) que informa o credenciamento das empresas de auditoria autorizadas a atuar na ICP-Brasil. Em planilha encaminhada pelo ITI no início dos trabalhos com dados sobre entidades credenciadas, consta a situação da empresa como “encerrada”.

189. Questionado sobre o período de atuação da empresa Crowe na ICP-Brasil, o ITI respondeu que a organização está credenciada desde 17 de abril de 2017, portanto está autorizada a realizar auditorias em AR desde abril de 2017 a abril de 2022, caso não haja renovação do credenciamento. Destacou que, por algum equívoco não identificado, a empresa de auditoria estava indevidamente com status no Sistema CASA como “encerrado”, quando deveria ser “credenciado”. Esse erro ocasionou a exclusão da empresa da publicação da página do ITI.

190. Em resposta à Solicitação de Auditoria nº 2, a Unidade concordou também com divergência de informação publicada na página do ITI relacionada à empresa Deloitte Auditores Independentes. A situação foi corrigida durante os trabalhos de campo.

191. Identificou-se ainda diferença entre os dados das informações encaminhadas em planilha sobre os Prestadores de Serviço de Suporte (PSS) credenciados e a lista divulgada no site da Unidade (<https://www.gov.br/iti/pt-br/assuntos/icp-brasil/lista-de-prestadores-de-servico-e-suporte-pss>). A Unidade explicou que às vezes ocorrem divergências por motivo de erro de cadastramento no Sistema CASA e os dados apresentados no sítio do ITI são oriundos desse sistema. Acrescentou que ao perceber divergências por meio da equipe ou alguma reclamação externa, as correções são realizadas no Sistema CASA.

192. Quanto aos dados dos PSSs, na oportunidade do questionamento, a Unidade informou que a correção das informações seria realizada com nova publicação na página do ITI, o que não foi observado até o momento.

193. Em manifestação após o relatório preliminar, a Unidade informou que foram corrigidas as inconsistências e as informações foram atualizadas. Acrescentou que será avaliada a possibilidade de melhorias para automatizar a publicação na página do ITI das informações referentes a PSS e empresas de auditoria.

194. A possível causa deste achado é a existência de falhas no cadastramento de informações no Sistema CASA, sem posterior fluxo de verificação para avaliar a conformidade dos dados inseridos na ferramenta, levando a não identificação de erros e permitindo publicações incompletas ou intempestivas no site da Unidade, com consequente comprometimento para o acesso à informação dos interessados e para o cumprimento dos requisitos de transparência.

195. Diante da necessidade de aperfeiçoar o processo de divulgação das informações proativamente disponibilizadas nos sítios eletrônicos institucionais, evitando o entendimento comprometido de informações de interesse público, mantém-se o registro do achado para acompanhamento das medidas de melhorias a serem implementadas.

10. Informação sobre as medidas adotadas pela Unidade para atender às exigências da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.

196. Questionada sobre as ações já realizadas para atendimento dos requisitos da Lei Geral de Proteção de Dados, o ITI citou as seguintes iniciativas:

- a) Por meio da Portaria nº 8, de 7 de fevereiro de 2020, alterada pela Portaria nº 40, de 10 de setembro de 2020, criou uma comissão de implementação da Lei Geral de Proteção de Dados Pessoais (LGPD), com os seguintes objetivos: analisar a lei e verificar sua aplicação no âmbito do ITI; estabelecer modelagem para implantação da governança de dados no ITI; coordenar junto aos departamentos/áreas do ITI o mapeamento dos dados e riscos associados; e apontar demais iniciativas para implementação da LGPD;
- b) Por meio da Portaria nº 58, de 17 de dezembro de 2020, em cumprimento ao inciso III do art. 23 e no art. 41 da Lei nº 13.709, de 14 de agosto de 2018 e às disposições do art. 1º da Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020, designou seu Encarregado pelo Tratamento de Dados Pessoais para o exercício das atribuições definidas na LGPD;
- c) Disponibilizou as informações do Encarregado pelo Tratamento de Dados Pessoais no sítio eletrônico do ITI;
- d) Por meio do Ofício nº 2/2021/GABIN/PRESIDENCIA-ITI, o Coordenador da Comissão de Implementação da LGPD apresentou os seguintes trabalhos realizados para o Senhor Diretor-Presidente do ITI:
 - i. Realizada análise da LGPD com vistas a verificar os pontos de aplicações no ITI;
 - ii. Iniciado o mapeamento dos dados e dos riscos associados ao tratamento de dados pessoais no âmbito do ITI;
 - iii. Nomeado o Encarregado pelo Tratamento de Dados Pessoais do ITI;
 - iv. Criado um espaço no site do ITI, como forma de comunicação com a sociedade, contendo os dados do Encarregado do ITI e, ainda em fase de desenvolvimento, temas relativos ao tratamento de dados pessoais no ITI;
 - v. Verificada a necessidade de inclusão do Encarregado pelo Tratamento de Dados Pessoais no Comitê de Governança Digital do ITI; e
 - vi. Definido, como metodologia de implementação da LGPD no ITI, o Guia de Boas Práticas para Implementação na Administração Pública Federal.

197. A Unidade ainda salientou que com a implantação do SEI os processos de credenciamento, fiscalização, entre outros, são classificados conforme o grau de necessidade aplicada a cada caso de sigilo às informações. Também se aplica a restrição de acesso a dados por meio da criação de diretório exclusivo de acesso à equipe lotada na CGAFI. Arquivos de dossiês de titulares de certificados são mantidos em diretórios restritos e são criptografados. As biometrias dos titulares de certificados são mantidas na sala cofre da AC Raiz.

198. Quanto à adequação das normas da ICP-Brasil às exigências da LGPD, analisando os normativos em vigor, observou-se que esses regulamentos ainda não apresentam referências à Lei nº 13.709/2018. Entretanto, acompanhou-se a publicação da Resolução CG ICP-Brasil nº 191, de 18 de maio de 2021, que instituiu Grupo de Trabalho Técnico – GTT destinado à elaboração de estudos e de propostas voltadas à adequação das normas da ICP-Brasil à Lei Geral de Proteção de Dados. O grupo tem prazo de 60 dias, prorrogáveis por igual período, para entrega de relatório com as conclusões e recomendações de alterações nos atos normativos.

199. Portanto, o ITI e o Comitê Gestor da ICP-Brasil estão ainda avançando nas ações para garantir conformidade com os ditames da Lei Geral de Proteção de Dados.

RECOMENDAÇÕES

200. Diante dos achados apresentados no corpo deste Relatório de Auditoria, apresentam-se a seguir as recomendações que visam auxiliar o gestor na implementação de melhorias nos processos analisados.

201. Para tanto, o ITI deverá apresentar a esta Ciset, no prazo de 30 dias após o recebimento do relatório definitivo, plano de ação, contendo, para cada recomendação indicada a seguir, as medidas a serem adotadas, o prazo para implementação e o responsável pelo desenvolvimento das ações, de modo a solucionar os achados apontados neste relatório, sem prejuízo de outras ações que, de igual modo, contribuam efetivamente para o aperfeiçoamento da gestão.

Achados nº 1, 2 e 3 (Credenciamento e manutenção do credenciamento de entidades)

1. Adotar procedimentos internos para aperfeiçoar o registro de informações gerenciais sobre motivos de descredenciamento, indeferimentos, fiscalizações realizadas, de modo a identificar padrões que revelem a necessidade de implementar medidas estruturantes no âmbito das entidades integrantes da ICP-Brasil;
2. Estabelecer controles periódicos adicionais dos critérios de credenciamento de entidades, com auxílio do cruzamento de bases de dados disponíveis, a fim de garantir a conformidade com o DOC-ICP-03, em complemento aos trabalhos de auditoria operacional realizados;
3. Solicitar providências das entidades indicadas no resultado de cruzamento de dados quanto à situação das pendências fiscais identificadas, a fim de garantir a manutenção do direito de atuação na ICP-Brasil, em conformidade com o DOC-ICP-03, adotando outras medidas regulamentares em caso de permanência das não conformidades;

Achado nº 4 (Controle dos relatórios de auditoria operacional)

4. Estabelecer controles adequados dos Planos Anuais de Auditoria Operacional e dos Relatórios de Auditorias Operacionais, de modo a cumprir as exigências do DOC-ICP-08, a manutenção dos critérios de credenciamento de entidades para operação regular junto à ICP-Brasil exigida no DOC-ICP-03, bem como permitir o acompanhamento de questões recorrentes nas entidades para que se possa adotar medidas estruturantes a todos os membros integrantes da cadeia de certificação digital;

Achado nº 6 (Cadastro de Agentes de Registro – CAR)

5. Estabelecer rotinas de acompanhamento e controle dos dados disponibilizados no Cadastro de Agentes de Registro (CAR), enquanto não seja possível implementar sistema informatizado para gestão do conjunto de dados, de modo a garantir confiabilidade na publicação das informações sobre os agentes autorizados a atuar na ICP-Brasil, conforme os termos da Instrução Normativa ITI nº 11, de 23 de outubro de 2020;

6. Apurar junto às Autoridades Certificadoras se os Agentes de Registro com indicação de falecimento no cadastro da Receita Federal e demais inconsistências identificadas nos cruzamentos de dados auxiliaram na emissão de certificados, a fim de que sejam adotadas providências junto às entidades envolvidas;

7. Exigir justificativas das entidades para o expressivo número de Agentes de Registro que não apresentam vínculo funcional na RAIS e permanecem atuando na ICP-Brasil, em desconformidade com as regras de segurança de pessoal definidas na IN ITI nº 10, de 22 de outubro de 2020, a fim que sejam adotadas providências para a não conformidade identificada;

8. Solicitar das entidades encarregadas da execução de auditorias operacionais na ICP-Brasil a análise sobre o cumprimento dos dispositivos normativos que tratam de segurança de pessoal, especialmente para o caso dos funcionários das serventias extrajudiciais que atuam como Agentes de Registro, a fim de que seja confirmado o atendimento das exigências normativas;

Achado nº 7 (Certificados digitais emitidos)

9. Aprimorar rotinas e métodos de acompanhamento dos dados encaminhados pelas Autoridades Certificadoras sobre a emissão de certificados, de modo a conseguir avaliar o cumprimento dos normativos da ICP-Brasil pelas entidades, bem como agir tempestivamente diante de possíveis casos de inconformidades ou fraudes;

10. Adotar melhorias na sistemática de envio automatizado dos dados dos certificados emitidos pelas Autoridades Certificadoras, de forma a permitir a adoção de instrumentos de verificação automática, integração de bases de dados, emissão de alertas para inconformidades, emissão de relatórios e de informações gerenciais pelo ITI;

11. Adotar providências para verificar as inconformidades apontadas nos resultados de cruzamento de dados apresentados, de forma a conferir o atendimento dos requisitos normativos

da ICP-Brasil pelos agentes envolvidos na cadeia de certificação, aplicando as medidas cabíveis em casos de confirmadas as irregularidades;

12. Rever as informações que devem ser enviadas semanalmente ao ITI sobre os certificados digitais emitidos, por força da IN ITI nº 5/2019, a fim de propor alteração normativa para inclusão de dados de Agentes de Registro que figuraram em cada processo de emissão, considerando a relevância da informação para as auditorias e fiscalizações realizadas pela AC Raiz;

13. Apresentar dados dos campos “Not after” e “Not before” a respeito dos casos identificados de certificados emitidos com data futura, a fim de comprovar a regularidade do procedimento adotado;

Achado nº 9 (Transparência)

14. Estabelecer rotina de acompanhamento das informações publicadas no sítio eletrônico da Unidade, de modo a identificar tempestivamente falhas nas publicações de interesse público.

CONCLUSÃO

202. O presente trabalho buscou avaliar o processo de certificação digital mantido e auditado pelo Instituto Nacional de Tecnologia da Informação – ITI, com ênfase no credenciamento e manutenção de entidades no âmbito da ICP-Brasil, bem como na implementação de rotinas e controles de informações encaminhadas pelas Autoridades Certificadoras, de forma a gerenciar o cumprimento dos normativos vigentes. Para cumprir os objetivos deste trabalho, elaborou-se matriz de planejamento, contendo questões de auditoria sobre os seguintes aspectos principais: credenciamento de entidades, manutenção de credenciamento, controles internos de informações e acompanhamento da implementação da LGPD.

203. O exame identificou que quanto ao processo de credenciamento sob responsabilidade do ITI, órgão executor das políticas de certificação, as orientações dos normativos estabelecidos pelo Comitê Gestor da ICP-Brasil estão sendo observadas. As auditorias pré-operacionais estão sendo realizadas para aferir o cumprimento das exigências constantes no DOC-ICP-03 e as análises são inseridas em processos acompanhados no Sistema SEI. A instrução dos processos de credenciamento também observa, de forma geral, as determinações normativas, seguindo o fluxo de trabalho definido pelo ITI. Os deferimentos e indeferimentos de credenciamento são precedidos de análises técnicas sobre o atendimento às condições do DOC-ICP-03. Pelas últimas alterações normativas, as análises de credenciamento não passam mais pela procuradoria jurídica da Unidade.

204. Quanto às auditorias operacionais, verificou-se que o ITI precisa aprimorar o acompanhamento do resultado dos trabalhos realizados pelas empresas de auditoria independente, com melhor controle sobre os Planos Anuais de Auditorias Operacionais e também sobre a manutenção dos critérios de credenciamento das entidades, a fim de ter disponíveis elementos para propor medidas estruturantes à cadeia de certificação. Constatou-se que existem entidades operando na ICP-Brasil sem comprovação da realização das auditorias operacionais anuais obrigatórias.

205. Observou-se durante as análises e cruzamento de dados que empresas ativas na ICP-Brasil apresentam pendências fiscais nem sempre identificadas pelos trabalhos das empresas de auditoria independente, deixando de ser atendidas exigências estabelecidas pelas resoluções do Comitê Gestor da ICP-Brasil. Não se mostra possível afirmar, portanto, que as auditorias operacionais estão sendo suficientes para verificar os requisitos de manutenção do credenciamento de entidades.

206. As empresas de auditoria independente passam por um processo de verificação de requisitos do DOC-ICP-08, a fim de conseguirem habilitação para realizar trabalhos na cadeia da ICP-Brasil. O ITI faz as verificações necessárias estabelecidas em normativo, checando as determinações para permitir o credenciamento dessas entidades. Entretanto, ainda se constatou a ausência, em um dos processos analisados, de documentos previstos nos itens 4.2 e 4.5 do DOC-ICP-08, que tratam do rol dos trabalhos realizados nos últimos dois anos pela empresa e da comprovação de que possuem corpo técnico de auditores com a experiência exigida, mas a situação foi sanada pela Unidade após o recebimento do relatório preliminar.

207. Quanto ao acompanhamento da regularização das não conformidades identificadas em relatórios de auditoria operacional e que ensejam recomendações à entidade auditada, verificou-se que o ITI adota as determinações do item 9 do DOC-ICP-08, definindo a participação das entidades subordinantes do PSCert auditado (AC vinculada à AR auditada) para controle das regularizações das inconformidades apresentadas em relatórios. Apenas para as auditorias com Conceito 4 (Inadequado) ou 5 (Inaceitável), o ITI inicia um processo para apuração e acompanhamento das não conformidades. Identificou-se, durante os trabalhos, caso de auditoria que apresentou resultado com Conceito 5 (Inaceitável), mas que o ITI não instaurou o processo de apuração na época devida, permitindo a continuidade da operação de entidade que não cumpre os critérios exigidos na legislação aplicável.

208. Em análise aos controles internos adotados pelo ITI para gerenciar informações encaminhadas pelas Autoridades Certificadoras e armazenadas em meios eletrônicos, buscou-se verificar a conformidade dos dados com as normas que regem a ICP-Brasil e as medidas implementadas em casos de inconsistências verificadas. Selecionaram-se as bases de dados de certificados emitidos em 2020 e 2021, bem como dados do Cadastro de Agentes de Registro – CAR, e conforme apresentado no corpo do relatório, após cruzamento de dados, visualizaram-se inconformidades que precisam ser aprofundadas pela Unidade, uma vez que o ITI atua como órgão responsável pela execução das normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, bem como pela execução de atividades de fiscalização e auditoria das entidades credenciadas e autorizadas a atuar na ICP-Brasil.

209. Os resultados dos cruzamentos de dados demonstram a existência de riscos para o processo de certificação digital que devem ser trabalhados pela Unidade. A busca por parcerias com órgãos governamentais para ampliar a troca de informações e aprimorar a análise de dados pode auxiliar no constante desenvolvimento de soluções para a segurança e confiança digital dos documentos e transações eletrônicas.

210. Como causas para os achados identificados durante o trabalho, podemos destacar: necessidade de melhorias das rotinas definidas para gerenciar a conformidade de dados encaminhados pelas Autoridades Certificadoras; equipe técnica reduzida para realizar as atribuições da CGAFI/DAFN; necessidade de aprimoramento de sistemas informatizados que atendam a rotinas

internas estratégicas; ausência de integração de bases de dados, tanto no que se refere a bases governamentais como bases de dados internas da Unidade.

211. Além das boas práticas implementadas pelo ITI para aprimoramentos do processo de credenciamento, importa destacar que a Unidade, em suas manifestações no decorrer deste trabalho, apresentou propostas de implementação de medidas que serão acompanhadas para solucionar as inconsistências descritas no relatório.

212. Entre os benefícios estimados desta auditoria, espera-se que a implementação de rotinas de testes automatizados em intervalos periódicos possa antecipar a visualização ágil de inconsistências nos dados acompanhados pela Unidade, permitindo a cobrança das devidas correções pelas autoridades responsáveis. Além da constante preocupação em sistematização das informações, com integração de bases de dados e padronização de dados para resgates rápidos de informações, as análises de medidas estruturantes para toda a cadeia de certificação mostram-se como chave para o fortalecimento da segurança da cadeia de certificação desde o credenciamento até a emissão de certificados.

213. As recomendações registradas neste relatório serão acompanhadas por meio de Plano de Providências Permanente da Unidade.

ANEXO

MANIFESTAÇÃO DA UNIDADE EXAMINADA E ANÁLISE DA EQUIPE DE AUDITORIA

A Unidade apresentou manifestação sobre o Relatório Preliminar por meio do Ofício nº 1/2021/PRESIDÊNCIA-ITI, de 27 de agosto de 2021, conforme registrado abaixo.

Achado nº 3 (Manutenção do credenciamento de entidades)

Manifestação da Unidade examinada

“Reconhecemos que realmente há necessidade de melhorias no controle anual de auditorias e a avaliação dos seus respectivos resultados. Estamos avaliando a melhor maneira de realizar cruzamento de dados de situação fiscal de forma a subsidiar e melhorar as ações de auditoria nas entidades da ICP Brasil.”

Análise da equipe de auditoria

Conforme manifestação apresentada pelo ITI, a Unidade concorda com o achado apresentado pela equipe de auditoria e reconhece a necessidade de adotar providências para melhorias.

Achado nº 4 (Controle dos relatórios de auditoria operacional)

Manifestação da Unidade examinada

“Reconhecemos que realmente há necessidade de melhorias no controle do planejamento anual de auditorias e a avaliação dos seus respectivos resultados. Até 2018 havia um sistema que fazia este tipo de controle, porém foi desativado por estar desatualizado. Está em elaboração um sistema para controle das auditorias realizadas anualmente nos Prestadores de Serviço de Certificação – PSC. A previsão para a implantação do sistema de controle de auditorias está prevista para dezembro de 2021. Por meio do sistema será possível a avaliação e cobrança dos resultados registrados nos relatórios das Empresas de Auditoria credenciadas junto ao ITI, bem como, será possível registrar o PLANO ANUAL DE AUDITORIA OPERACIONAL (PLAAO), avaliação e cobrança dos resultados registrados nos relatórios das Empresas de Auditoria credenciadas junto ao ITI.”

Análise da equipe de auditoria

Conforme manifestação apresentada pelo ITI, a Unidade concorda com o achado apresentado pela equipe de auditoria e reconhece a necessidade de adotar providências para melhorias.

Achado nº 6 (Cadastro de Agentes de Registro – CAR)

Manifestação da Unidade examinada

- a) Não comprovação de vínculo funcional entre 15.477 Agentes de Registro (AGR) e as respectivas Autoridades de Registro (AR) credenciadas junto à ICP-Brasil.

“O que é a ARPEN?

Associação dos Registradores de Pessoas Naturais do Estado de São Paulo. Fundada em fevereiro de 1994, a Associação dos Registradores de Pessoas Naturais do Estado de São Paulo (Arpen-SP) representa os 836 cartórios de registro civil, que atendem a população em todos os 645 municípios do Estado, além de estarem presentes em outros 169 distritos e subdistritos, realizando os principais atos da vida civil de uma pessoa: o registro de nascimento, casamento e óbito.

O que é a AR CNBSP:

Artigo 1º - O Colégio Notarial do Brasil – Seção de São Paulo doravante designado simplesmente “Colégio”, “Entidade” ou “Associação”, é uma associação civil sem fins econômicos, constituída em 9 de janeiro de 1951, filiada ao Colégio Notarial do Brasil, dotada de competência e autonomia administrativa, patrimonial e representativa em todo o Estado de São Paulo, e com sede e foro na cidade de São Paulo, Capital, sendo indeterminado o seu prazo de duração. (Estatuto CNBSP)

O que diz os normativos da ICP-Brasil:

3.2.2 As serventias extrajudiciais autorizadas pelo Conselho Nacional de Justiça, nos termos do art. 236 da Constituição Federal, desde que formalmente vinculadas a uma AR já credenciada, poderão ter seus funcionários habilitados que exercem a atividade de agentes de registro. (DOC-ICP-03-versão 7.0)

Obs: não há vínculo empregatício diretamente com a ARPEN e a CNBSP. O cartório é um associado e a norma permitem que seus funcionários exerçam a função de AGR. Portanto, entende-se equivocada a análise e apontamento de irregularidade nos 1451 AGRs da AR ARPEN e nos 489 AGRs CNBSP sem vínculo empregatício.

Existe a situação em que a AR é uma microempresa e o empresário é o AGR. Neste caso não há relação de emprego.”

Análise da equipe de auditoria

Considerando o posicionamento da Unidade e em razão do que dispõe o item 3.2.2 do DOC-ICP-03 sobre as serventias extrajudiciais, esta equipe de auditoria retirou do Quadro 3 o quantitativo de AGRs relacionados à AR ARPEN SP e à AR CNBSP. Entretanto, é relevante acompanhar as exigências de habilitação dos funcionários de cartórios como agentes de registro, uma vez que se verificou ausência de vínculos funcionais da maioria dos CPFs indicados no cadastro, seja com as associações ou mesmo com os cartórios, o que requer avaliação sobre as características de segurança exigidas das entidades, conforme dispositivos do DOC-ICP-03.01.

A conferência dos requisitos de segurança de pessoal deve ser analisada no âmbito das auditorias operacionais realizadas nas entidades da ICP-Brasil, a fim de verificar a conformidade com os normativos aplicáveis.

A evidenciação de elevado percentual de não cumprimento da regra que impõe a necessidade de vínculo empregatício dos Agentes de Registro gera alerta para a implementação de procedimentos de controle complementares sobre o CAR, antes da ampla divulgação no sítio do ITI das informações cadastrais dos agentes que atuam no âmbito da ICP-Brasil, bem como cobrança de justificativas junto às empresas que executaram as auditorias operacionais nas entidades para apresentar esclarecimentos sobre este achado.

- b) Identificação de 25 Agentes de Registro falecidos, 1 menor de idade, 3 com CPFs não válidos e 4 maiores de 80 anos sem vínculo trabalhista na relação do Cadastro de Agentes de Registro – CAR.**

Manifestação da Unidade examinada

“Reconhecemos a necessidade de melhorias no controle de AGRs. Novas regras automatizando a análise dos dados recebidos serão implantadas.

Porém, discordamos da quantidade de 17.417 Agentes de Registro devido a imprecisão na pesquisa elaborada por essa equipe de auditoria.”

Análise da equipe de auditoria

Conforme manifestação apresentada pelo ITI, a Unidade concorda com a necessidade de melhorias no Cadastro de Agentes de Registro – CAR, razão pela qual o registro foi mantido para acompanhamento.

- c) Manutenção de 333 Agentes de Registro na base de dados do CAR com vinculação a Autoridades de Registro (AR) descredenciadas ou indeferidas.**

Manifestação da Unidade examinada

“Reconhecemos a necessidade de melhorias no controle de AGRs. Diversas melhorias já foram implementadas pela CGNPE/DAFN para aprimorar a validação dos dados apresentados pela AC/AR, vide Ofício Circular nº 03/2021/DAFN-ITI (em anexo)

Novas regras automatizando a análise dos dados recebidos serão implantadas.”

Análise da equipe de auditoria

Conforme manifestação apresentada pelo ITI, a Unidade concorda com o achado apresentado pela equipe de auditoria. Mantém-se o registro para acompanhamento das melhorias a serem implementadas.

Achado nº 7 (Certificados digitais emitidos)

- a) Emissão de 11.545 certificados digitais com participação de Autoridade de Registro com inscrição do CNPJ baixada.**

Manifestação da Unidade examinada

“O Achado não é procedente. No arquivo disponibilizado com 2.422 registros, apenas 201 certificados possuíam data de emissão posterior a data de baixa na RFB. Pode ser constatado observando a coluna J (teste1) VERDADEIRO. Os demais 2.221 possuem situação FALSO na referida coluna, que significa emissão do certificado em data anterior a data de baixada na RFB. Quanto aos 201 “VERDADEIRO” testei 05 cinco primeiros da lista e todos foram emitidos por “Certificado digital” que significa RENOVAÇÃO DE CERTIFICADO. A Renovação ocorre quando o titular possui um certificado válido e faz uso do mesmo para emitir um novo certificado, sem a participação da

Autoridade de Registro no processo de emissão. Portanto, não é correto a afirmativa de que houve emissão de certificados digitais com a participação de AR com inscrição baixada.”

Análise da equipe de auditoria

Conforme indicado no texto do achado, foram realizados testes complementares que totalizam o quantitativo de 11.545 certificados emitidos com o registro de empresas com inscrição do CNPJ baixada. A planilha com o resultado dos testes complementares será encaminhada à Unidade. Vale aqui novamente destacar que os itens apresentados neste relatório demandam procedimentos de checagem complementar pelo ITI para avaliar situações específicas, a fim de validar o alerta indicado e permitir identificar a necessidade de medidas estruturantes dentro da cadeia de certificação digital. O ITI poderá apresentar as conferências realizadas no âmbito do documento “Plano de Ação” a ser apresentado, conforme disposto no tópico Recomendações deste relatório.

b) Registro de emissão de 25 certificados digitais para titulares falecidos

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e será necessário apuração individualizada por parte da AC. Neste momento, estamos em ajustes finais para o acesso à base do BCPF mantida pela RFB e será possível futuramente a adoção de rotina para verificação desta situação detectada pela equipe de auditoria.

Importante destacar que todos os 25 certificados emitidos foram na modalidade de ‘certificado digital’ que significa foi reemissão utilizado o certificado digital válido emitido possivelmente antes do óbito. Nessa situação não há não conformidade da AC ou AR, pois não é possível aos entes da ICP Brasil realizar o batimento com a base de óbito. Ressaltamos que os critérios de análise dessa equipe de auditoria devem considerar a situação de reemissão.”

Análise da equipe de auditoria

Conforme informado pela Unidade, os casos constatados ocorreram em situação de renovação do certificado, o que requer análise sobre medidas de controle para situações como as identificadas neste item. Salienta-se a necessidade de acordo entre o ITI e a Secretaria Especial da Receita Federal do Brasil para compartilhamento de dados, de modo a permitir a verificação da ocorrência de casos de falecimento, impedir a emissão de novas certificações utilizando os dados de pessoa falecida, bem como providenciar as medidas de cancelamento dos certificados vigentes.

c) Certificados emitidos que apresentam nomes de titulares diferentes para um mesmo CPF.

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e será necessário apuração individualizada por parte da AC. Neste momento estamos em ajustes finais para o acesso à base do BCPF mantida pela RFB e será possível futuramente a adoção de rotina para verificação desta situação detectada pela equipe de auditoria. Atualmente não é possível fazer batimento com a base de CPF da RFB. A base de certificado deve refletir tão somente os dados recebidos das AC e reafirmamos não há erro no cadastro. Por fim nos dados apresentados dos 789 certificados, em uma análise preliminar foi

possível identificar algumas inconsistências nos dados apresentados que não permitem afirmar que há nomes diferentes para todos os casos, cito um exemplo. Salientamos que uma pessoa pode alterar seu nome pelo casamento, motivos pessoais, mudança de sexo, etc e que essa equipe de auditoria deveria levar em consideração essas situações.”

Análise da equipe de auditoria

Considerando as manifestações da Unidade, diante da responsabilidade por realizar auditorias e fiscalizações, identificando possíveis irregularidades na emissão dos certificados, convém que os casos apresentados nos resultados dos cruzamentos sejam analisados para que as exigências dos normativos da ICP-Brasil sejam cumpridas, principalmente quanto à correta identificação do responsável pelo certificado, que é a base da segurança da certificação digital. Ademais, medidas de controle também precisam ser revistas para avaliar a ocorrência de erros de cadastro e proporcionar proteção razoável às operações.

d) Ausência de informações sobre as Autoridades de Registro (AR) responsáveis pelo encaminhamento de solicitações de emissão de certificados em mais de 50 mil registros.

Manifestação da Unidade examinada

“A ausência do nº do CNPJ pode representar uma não conformidade no certificado digital, contudo, já existe rotina implementada na CGAFI para avaliar esse requisito. Nas rotinas de importação de certificado é executado uma etapa de avaliação de conformidade que verifica diversos itens com o objetivo de manter a padronização dos certificados ICP Brasil e sempre que ocorre a ausência do CNPJ no local exigido as AC são comunicadas para a correção futura em seus procedimentos de emissão de certificado (template), sem a revogação do certificado. Mas diante da indicação da auditoria Ciset analisamos por amostragem os dados apresentados como as seguintes constatações:

- 845 certificados – não se aplica – São certificados SSL, e TS para uso em equipamento e aplicação e possuem restrições técnicas para o uso.
- Testamos 12 registros apresentados pela equipe de auditoria 1.7_ArnoPreenchida e verificamos que todos foram por meio de Certificado digital, que corresponde a Renovação eletrônica, portando não é aplicável o CNPJ da AR.

(...)

Diante desta constatação pode ter ocorrido que durante o cruzamento de dados, não foi considerado no CN do certificado o tipo de emissão ‘Certificado digital’ ou ‘Renovação eletrônica’. Solicitamos que seja reconsiderado o apontamento.”

Análise da equipe de auditoria

Importa destacar que os cruzamentos realizados sobre dados de certificados digitais emitidos em 2020 e 2021 foram realizados com base nas informações fornecidas à equipe de auditoria. É preciso que a Unidade examine os resultados para considerar eventuais inconsistências e casos específicos que não se aplicam à questão apontada. Conforme consta no tópico “Recomendações” deste relatório, o ITI deverá adotar providências para verificar as inconformidades, validar os dados dos alertas e aplicar as medidas cabíveis para os casos de irregularidades confirmadas.

e) Certificados emitidos com atuação de Autoridades de Registro (AR) que apresentam inconsistências no assentamento dos vínculos empregatícios de Agentes de Registro.

Manifestação da Unidade examinada

“As questões relacionadas a AGR já foram tratadas no item 7. Fragilidades nas informações divulgadas no Cadastro de Agentes de Registro – CAR.”

f) Certificados emitidos com data futura

Manifestação da Unidade examinada

“A emissão de certificado com data futura tem previsão normativa e não oferece risco a credibilidade ou a segurança do processo de certificação digital. Os certificados com data futura têm o seu uso impossibilitado por qualquer aplicação que faz uso do certificado, pela existência dos campos Not after e Not before.

DOC ICP 05 - 3.2.3.1.3 Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais dos entes federativos, deverão ser verificados: a) por agente de registro distinto do que realizou a etapa de identificação; Infraestrutura de Chaves Públicas Brasileira Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil DOC-ICP-05 - versão 6.1 24 b) pela AR ou AR própria da AC ou ainda AR própria do PSS da AC; e c) antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

Solicitamos que seja reconsiderado o apontamento por não haver desconformidade”.

Análise da equipe de auditoria

Apesar da Unidade não considerar o apontamento como desconformidade, mantém-se o registro da situação encontrada para que seja atendida recomendação de apresentar os valores que indicam as diferenças de datas referentes à emissão do certificado e ao período que podem efetivamente ser utilizados (“Not after” e “Not before”).

g) Outras situações identificadas na base de dados de certificados emitidos.

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e reafirmamos que não há fragilidade na base de dados. Reafirmamos que Base de Certificados tem objetivo de espelhar fielmente os dados encaminhados pela AC.”

Análise da equipe de auditoria

Diante dos esclarecimentos prestados, destaca-se que a ausência de integração com outras bases de dados não permite a geração de alertas às autoridades da cadeia de certificação para indicar

cadastros inconsistentes e impedir a continuidade do processo de emissão diante da constatação de inconformidades. Ademais, destaca-se a necessidade de aprimorar as rotinas implementadas pelo ITI para controle dos dados encaminhados pelas Autoridades Certificadoras, de forma a confirmar o atendimento das normas da ICP-Brasil.

Manifestação da Unidade examinada sobre as recomendações propostas para o Achado nº 7

“Em relação as recomendações solicitamos reconsiderar no todo ou em parte, diante dos esclarecimentos pontuais apresentados no item 8 - Certificados digitais emitidos (de ‘a’ a ‘j’) e ainda: 1. Já existe rotina implementada pela CGAF, de com bom nível de maturidade, para avaliação da conformidade dos certificados digitais encaminhados semanalmente pelas AC, vide print em anexo (Envio de certificados e biometrias · Wiki · SGC2 · GitLab); 2. Existe rotina implementada para detecção e contenção de fraude, que consiste em cruzamento de dados de certificados (SGC2), dados de fraude (SAF) e CASA. Essa rotina consiste em obtenção de alertas possível fraude, que são apuradas e quando há indícios consistentes são encaminhados para averiguação da AC – vide exemplo de relatório em anexo (20210810_AC_CERTISIGN_RFB_fraude); 3. Existe rotina de acompanhamento de conformidade dos certificados digitais com foco em manutenção do padrão e atendimento das normas quanto ao formato do certificado. Assim sendo diversos itens são avaliados semanalmente e gerado Relatório de ERRO, que são encaminhados para as AC, que apresentam os esclarecimentos e realiza as correções Vide Exemplo, em anexo: (2020-01-13_2020-01-19_Relatório de Conformidade e Relatório Geral de Conformidade - Novembro-2020). Por fim, entendemos todo e qualquer processo necessita de contínuo aprimoramento, isso se aplica também e de verificação de conformidade e detecção de fraude. Já identificamos algumas melhorias a serem implementadas que atendem as sugestões da Ciset, como o batimento com os dados de obtido utilizando a base da RFB e de situação de credenciamento das AR/AC (Descredenciado, Indeferido, penalizadas etc.) no cadastro de ITI (CASA)”.

Análise da equipe de auditoria

Diante das rotinas já implementadas pela Unidade e a necessidade de contínuas melhorias, consideramos nas recomendações deste relatório a necessidade de aprimoramento das medidas de acompanhamento dos dados encaminhados pelas Autoridades Certificadoras, de modo a melhor avaliar o cumprimento dos normativos da ICP-Brasil.

Achado nº 8 (Observações sobre dados de certificados digitais emitidos)

a) Multiplicidade de certificados emitidos para um mesmo CPF

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e reafirmamos que não há necessidade de estabelecimento de rotina para avaliar a quantidade de certificado emitido por usuário. A decisão de adquirir um ou mais certificados é exclusiva do usuário que compra e paga pela aquisição. A Lei, MP 2.200/2001 afirma que ‘O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento’, portanto não cabe ao ITI ou as AC saber qual a necessidade de uso pelo seu titular.”

b) Ausência do número de CPF do titular em 18 certificados emitidos.

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e reafirmamos que não há necessidade de incluir obrigatoriamente o CPF como obrigatório no certificado digital. Conforme já apresentado, o normativo não define como obrigatório o CPF, mas, define como obrigatório o nome completo e a data de nascimento. ‘DOC ICP 05 item 3.2.3.2.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados: a) nome completo, sem abreviações;1 b) data de nascimento.’ Solicitamos que seja reconsiderado o apontamento.”

c) Emissão de certificados para titulares maiores de 90 anos

Manifestação da Unidade examinada

“Mantemos os esclarecimentos já prestados e reafirmamos que não há necessidade de incluir controles adicionais para análise de idade, pois o risco supostamente existe maior de óbito, considerando a expectativa de vida, contudo esse controle é suprido por outra análise.”

Análise da equipe de auditoria

Os itens foram mantidos como informação no relatório, considerando a necessidade de acompanhamento e aprimoramento constante dos requisitos de segurança nas operações de emissão de certificados digitais, apesar de inicialmente os itens não terem sido apontados como fatores de riscos para as operações.

Achado nº 9 (Transparência)

Manifestação da Unidade examinada

“Foram corrigidas as inconsistências e as informações atualizadas. Será avaliada a possibilidade de melhorias para automatizar a publicação na página do ITI das informações referentes a PSS e empresas de auditoria.”

Análise da equipe de auditoria

Diante da necessidade de aperfeiçoar o processo de divulgação das informações proativamente disponibilizadas nos sítios eletrônicos institucionais, evitando o entendimento comprometido de informações de interesse público, mantém-se o registro do achado para acompanhamento das medidas de melhorias a serem implementadas.