MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Instituto Nacional de Tecnologia da Informação - ITI
SCN QUADRA 02 BLOCO E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3945 - www.gov.br/iti/pt-br

NOTA TÉCNICA Nº 3/2025/CGNPE/DAFN

PROCESSO Nº 00100.000280/2025-94

INTERESSADO: COMITÊ GESTOR DA ICP-BRASIL

1. ASSUNTO

1.1. Pauta a ser deliberada pelo Comitê Gestor da ICP-Brasil, por meio de resolução, acerca de alterações na Resolução CG ICP-Brasil nº 179 (DOC-ICP-04) decorrentes da Pauta Modernizante.

2. SÍNTESE DO PROBLEMA

2.1. A Pauta Modernizante da ICP-Brasil, aprovada pela Resolução CG ICP-Brasil nº 211, organizou os campos e extensões dos perfis dos certificados da ICP-Brasil em um novo formato de tabelas para facilitar a compreensão e aplicação. Contudo, foi identificado um problema na indicação do campo *Subject Key Identifier* de algumas dessas tabelas, que foi replicado para certificados de usuário final, quando deveria ser indicado apenas para certificados de Autoridade Certificadora.

2.2. Além disso, verificou-se que em alguns trechos do DOC-ICP-04 há referência ao certificado de sigilo que foi excluído pela Resolução CG ICP-Brasil nº 211. Para garantir a coerência normativa e evitar ambiguidades, torna-se necessária a correção dessas inconsistências.

2.3. Como correção, propõe-se a revogação do campo indevido nas tabelas pertinentes e a adequação do regulamento quanto à exclusão do certificado de sigilo. A medida requer aprovação do Comitê Gestor da ICP-Brasil por meio de nova resolução, dada a necessidade de alteração de conteúdo normativo

3. CONTEXTUALIZAÇÃO

3.1. A Resolução CG ICP-Brasil nº 211, aprovada em 31 de outubro de 2024, introduziu mudanças significativas em relação aos tipos de certificados da ICP-Brasil. No escopo dessas alterações, foi realizada uma avaliação sobre os perfis dos certificados adotados pela ICP-Brasil e a forma como estavam apresentados nos normativos.

3.2. Visando facilitar a compreensão sobre o perfil detalhado de cada tipo de certificado, foi constatada a necessidade de adequar a redação dos dispositivos que tratavam dos campos e das extensões dos certificados de usuário final, de Autoridade Certificadora e da Lista de Certificados Revogados – LCR, que estavam dispostos em itens diferentes dos DOC-ICP-04 e 05, de forma a reuni-los em um esquema de tabelas, possibilitando a pronta identificação de cada perfil.

3.3. Dessa maneira, a Resolução nº 211 acrescentou o Anexo I ao DOC-ICP-04 com 09 (nove) tabelas detalhando os seguintes campos e extensões:

I - Certificado de Assinatura Digital para Pessoa Física;

II - Certificado de Selo Eletrônico para Pessoa Jurídica;

III - Certificado de Equipamento de Carimbo do Tempo;

IV - Certificado de Aplicações Específicas;

V - Certificado de Equipamento OM-BR;

VI - Certificado de Equipamento SAT;

VII - Certificado de AC que emite certificado para outras AC;

VIII - Certificado de AC que emite certificado para usuário final; e

IX - Campos e extensões das Listas de Certificados Revogados (LCR).

3.4. As discussões que antecederam a aprovação desse regulamento envolveram o corpo técnico do ITI, outros órgãos de governo, entidades do mercado de certificação digital e a sociedade civil em geral, por meio de consulta pública. Contudo, apenas em 26 de dezembro de 2024 foi constatado que poderia haver um equívoco em relação a campo *Subject Key Identifier* descrito nas tabelas.

3.5. Inicialmente, a AC JUS apontou que as tabelas do DOC-ICP-04 estavam indicando que no campo *Subject Key Identifier* deveria conter "Hash 160 bits SHA-1 da chave pública da AC titular do certificado". Enquanto essa indicação é correta apenas para certificado de AC. Portanto a indicação estava incorreta nas tabelas de certificados de usuário final. Para usuário final, se o campo existir, deve conter a informação "Hash 160 bits SHA-1 da chave pública do certificado"

3.6. Em discussão interna sobre a retificação do ato normativo, restou confirmado que a ICP-Brasil não adotava o campo *Subject Key Identifier* para os certificados de usuário final, apenas para os certificados de Autoridade Certificadora. Contudo indicava, e continua indicando, que "outros campos de extensão poderão ser utilizados na forma e propósitos definidos, conforme RFC5280". Ou seja, não proíbe sua implementação.

3.7. A fim de manter a definição já estabelecida pela ICP-Brasil sobre o campo *Subject Key Identifier,* faz-se necessário revogar esse campo nas tabelas de perfil de certificado de usuário final 1 (Certificado de Assinatura Digital de Pessoa Física), 2 (Certificado de Selo Eletrônico para Pessoa Jurídica), 3 (Certificado de Equipamento de Carimbo do Tempo), 5 (Certificado de Equipamento OM-BR) e 6 (Certificado de Equipamento SAT).

3.8. A tabela de perfil de certificado nº 4 (Certificado de Aplicações Específicas) não indica o campo *Subject Key Identifier.* As tabelas 7 e 8 são de certificado de Autoridade Certificadora, portanto estão corretas e devem ser mantidas. A tabela 8 corresponde a campos e extensões de LCR e não tem o campo *Subject Key Identifier.*

3.9. Ao apresentar a proposta de retificado ao Procurador Chefe do ITI, foi orientado que tal correção deveria se dar por nova resolução do Comitê Gestor, uma vez que trata-se de uma alteração de conteúdo e não apenas uma correção de erro formal. A sugestão foi acatada.

3.10. Adicionalmente, a fim de sanar uma omissão na Resolução CG ICP-Brasil nº 211, que deixou de aplicar no DOC-ICP-04 alteração condizente com a extinção do certificado de sigilo em alguns itens específicos, foi incluída na proposta em questão a alteração nos seguintes itens:

"6.2.4.2 A AC responsável pela PC não poderá manter cópia de segurança de

chave privada de titular de certificado de assinatura digital por ela emitido, salvo nos casos em que esta é credenciada como PSC. ~~Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC poderá manter cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido~~.

...

6.2.5 Arquivamento de chave privada

6.2.5.1 ~~Neste item de uma PC que defina certificados de sigilo, devem ser descritos, quando cabíveis, os requisitos para arquivamento de chaves privadas.~~ Não devem ser arquivadas chaves privadas de assinatura digital.

...

6.3.2.2 Caso a PC se refira a certificados de sigilo, ela deve definir os períodos de uso das chaves correspondentes." REVOGAR

3.11. Cabe destacar que essas alterações são reflexo do que já foi estabelecido pela Resolução CG ICP-Brasil nº 211 e foram igualmente aplicadas por esse regulamento no DOC-ICP-05. Destaca-se também que essa proposta de correção foi objeto de análise jurídica, sendo aprovada pelo PARECER n. 00001/2025/PROFE/PFE-ITI/PGF/AGU (SEI 0718150).

3.12. Inicialmente, a correção em relação ao certificado de sigilo no DOC-ICP-04 compunha a proposta de pauta de alteração do prazo máximo de validade do certificado de Selo Eletrônico em Hardware - SE-H, tratada no processo SEI nº 00100.003588/2024-19, que seria apresentada na primeira reunião ordinária do Comitê Gestor. Contudo, em decorrência da urgência de emissão do certificado da AC MRE, para viabilizar a emissão e distribuição do certificado que assina o passaporte brasileiro em tempo hábil para garantir o prazo de vigência de 10 anos do passaporte assinado com certificado ICP-Brasil, foi convocada uma reunião extraordinária emergencial para o dia 30 de janeiro de 2025 para deliberar especificamente sobre o tema urgente. Assim os temas foram separados.

4. ANÁLISE DE IMPACTO REGULATÓRIO

4.1. Foi realizada a análise do problema regulatório aqui apresentado, qual seja uma correção normativa, e da medida proposta para solucioná-lo à luz do Decreto nº 10.411, de 30 de junho de 2020, o qual regulamenta a análise de impacto regulatório e indica os casos de obrigatoriedade, inaplicabilidade ou de dispensa de AIR, a saber:

> Art. 1° Este Decreto regulamenta a análise de impacto regulatório, de que tratam o art. 5º da Lei nº 13.874, de 20 de setembro de 2019 e o art. 6º da Lei nº 13.848, de 25 de junho de 2019, e dispõe sobre o seu conteúdo, os quesitos mínimos a serem objeto de exame, as hipóteses em que será obrigatória e as hipóteses em que poderá ser dispensada.
>
> .....
>
> § 2º O disposto neste Decreto aplica-se às propostas de atos normativos formuladas por colegiados por meio do órgão ou da entidade encarregado de lhe prestar apoio administrativo.
>
> .....
>
> Art. 3º A edição, a alteração ou a revogação de atos normativos de interesse geral de agentes econômicos ou de usuários dos serviços prestados, por órgãos e entidades da administração pública federal direta, autárquica e fundacional será precedida de AIR.
>
> .....
>
> § 2º O disposto no **caput não se aplica** aos atos normativos:

I - de natureza administrativa, cujos efeitos sejam restritos ao âmbito interno do órgão ou da entidade;

II - de efeitos concretos, destinados a disciplinar situação específica, cujos destinatários sejam individualizados;

III - que disponham sobre execução orçamentária e financeira;

IV - que disponham estritamente sobre política cambial e monetária;

V - que disponham sobre segurança nacional; e

VI - que visem a consolidar outras normas sobre matérias específicas, sem alteração de mérito.

Art. 4º **A AIR poderá ser dispensada**, desde que haja decisão fundamentada do órgão ou da entidade competente, nas hipóteses de:

I - urgência;

II - ato normativo destinado a disciplinar direitos ou obrigações definidos em norma hierarquicamente superior que não permita, técnica ou juridicamente, diferentes alternativas regulatórias;

III - ato normativo considerado de baixo impacto;

IV - ato normativo que vise à atualização ou à revogação de normas consideradas obsoletas, sem alteração de mérito;

.....

VI - ato normativo que vise a manter a convergência a padrões internacionais;

VII - ato normativo que reduza exigências, obrigações, restrições, requerimentos ou especificações com o objetivo de diminuir os custos regulatórios; e

VIII - ato normativo que revise normas desatualizadas para adequá-las ao desenvolvimento tecnológico consolidado internacionalmente, nos termos do disposto no Decreto nº 10.229, de 5 de fevereiro de 2020.

4.2. Considerando que a proposta visa sanar incoerências em relação a definições já estabelecidas na ICP-Brasil, concluiu-se pela dispensa de AIR com base no disposto nos incisos III e VII do art, 4°, por tratar-se de ato normativo considerado de baixo impacto e que reduz exigências, obrigações, restrições, requerimentos ou especificações com o objetivo de diminuir os custos regulatórios.

5. PROVIDÊNCIAS PROPOSTAS

5.1. Alteração do DOC-ICP-04 para corrigir a indicação indevida do campo *Subject Key Identifier* nas tabelas dos certificados de usuário final.

5.2. Adequação dos trechos do DOC-ICP-04 que fazem referência ao certificado de sigilo, adequando o regulamento à Resolução CG ICP-Brasil nº 211.

6. CONCLUSÃO

6.1. Considerando os apontamentos feitos, propõe-se a submissão de proposta de resolução ao Comitê Gestor da ICP-Brasil para alterar o anexo da Resolução CG ICP-Brasil nº 179 (DOC-ICP-04) para corrigir a indicação do campo *Subject Key Identifier,* bem como para adequá-lo à extinção do certificado de sigilo.

Documento assinado eletronicamente por **Luciana Cristina Correa de Siqueira**, **Coordenador-Geral de Normalização e Pesquisa**, em 31/01/2025, às 19:14, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 478522979806018209293085645 2

A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0721090** e o código CRC **CD4EF577**.

Referência: Processo nº 00100.000280/2025-94 SEI nº 0721090