PAUTA 06

Descontinuidade de emissão de certificados do tipo SSL/TLS para identificação pelos navegadores de internet

1. Síntese do problema ou da situação que reclama providências.

O ITI realizou análise técnica sobre a viabilidade e aplicabilidade dos certificados digitais do tipo SSL/TLS ICP-Brasil, que indicou inviabilidade de manutenção desse tipo de certificado digital no âmbito da ICP-Brasil.

Esse estudo concluiu que há:

a) questões de incompatibilidade do modelo internacional de hierarquia com entidade única em relação a múltiplas entidades, no caso da ICP-Brasil, inviabilizando a governança exigida no âmbito do CA/B Fórum e normas *WebTrust*;

b) afetação de insegurança para os provedores de serviço e para os usuários desses serviços devido aos alertas de segurança emitidos por navegadores web, seja pela ausência da raiz da ICP-Brasil no repositório confiável dos navegadores ou por outros fatores alheios à ICP-Brasil;

c) baixa representatividade (0,02% do total de certificados válidos na ICP-Brasil) desse tipo de certificado digital utilizado atualmente no mercado brasileiro;

d) ausência de recomendação ou exigência de que os sítios de internet de governo utilizem certificados digitais do tipo SSL/TLS padrão ICP-Brasil em seus sítios ou serviços de Internet (Decreto n° 3.996/2001 foi revogado);

e) alternativas de certificados SSL/TLS fora da ICP-Brasil com nível de segurança equivalente, com ampla disponibilidade no mercado e, em alguns casos, de forma gratuita.

Importante destacar que se trata tão somente de certificados SSL/TLS, da cadeia v10, da AC Raiz da ICP-Brasil, destinados àqueles que necessitam de reconhecimento confiável exclusivamente pelos navegadores de internet (*browsers*), tais como Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Opera e outros.

Destaca-se também que a cadeia v10 da AC Raiz da ICP-Brasil será mantida para emissão exclusiva de certificados digitais SSL/TLS para aplicações especiais, ou seja, aplicações específicas, a exemplo do Sistema *Open Finance* Brasil (OFB), Sistema *Open Insurance* Brasil (OIB), Sistema de Pagamentos Brasileiro (SPB), dentre outros. Entende-se por aplicações especiais ou específicas aquelas realizadas entre entidades restritas, em um ecossistema fechado, onde a dependência de reconhecimento confiável pelos navegadores não é relevante, visto que suas autenticações são mútuas e restritas aos intervenientes conhecidos.

A descontinuidade, a partir do momento em que for efetivada, implicará num período de transição de 1 (um) ano ainda com certificados SSL/TLS ICP-Brasil vigentes, dado que esta é a vigência dos certificados dessa natureza, porém, novas emissões desses certificados devem cessar de imediato à publicação da resolução que aprovar sua descontinuidade pela ICP-Brasil.

2. Soluções e providências contidas no ato normativo.

Resolução do Comitê Gestor para determinação da descontinuidade de emissão de certificados SSL/TLS, no âmbito da ICP-Brasil, destinados àqueles que necessitam de reconhecimento confiável

exclusivamente pelos navegadores de internet (*browsers*), tais como Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Opera e outros.

Fica mantida a cadeia v10 da ICP-Brasil exclusivamente para emissão de certificados digitais SSL/TLS para aplicações específicas, a exemplo do Sistema *Open Finance* Brasil (OFB), Sistema *Open Insurance* Brasil (OIB), Sistema de Pagamentos Brasileiro (SPB), dentre outros. Entende-se por aplicações específicas aquelas realizadas entre entidades restritas, em um ecossistema fechado, onde a dependência de reconhecimento confiável pelos navegadores não é relevante visto que suas autenticações são mútuas e restritas aos intervenientes conhecidos.

3. Alternativas existentes às medidas propostas.

Não há alternativas existentes à medida ora proposta.

4. Custos.

Não há custo ao ITI associado à medida.

As AC subsequentes à AC Raiz incorrerão em custos operacionais para adequação de suas PC e DPC relacionadas ao tipo de certificado em descontinuidade. Impacto na comercialização desse tipo de certificado a ser descontinuado não é significativo, conforme a baixa representatividade (0,02%) no mercado de certificados digitais.

5. Razões que justificam a urgência.

O impacto da descontinuidade neste momento somente refletirá de forma efetiva após 1 (um) ano da data da aprovação da descontinuidade. Isso ocorre devido à possibilidade de emissão de certificado em data prévia à vigência da descontinuidade e esse certificado emitido possuir prazo de validade de um ano, estendendo demasiadamente o problema.

6. Impacto/Riscos sobre as Operações da ICP Brasil.

O impacto é mínimo devido à baixa representatividade desse tipo de certificado no mercado de certificados digitais.

Não há riscos sobre as operações da ICP-Brasil.

7. Análise de Impacto Regulatório

Para implementação da proposta em questão, a minuta de Resolução do Comitê Gestor da ICP-Brasil deve observar o Decreto nº 10.411, de 30 de junho de 2020, o qual regulamenta a análise de impacto regulatório, indicando os casos de obrigatoriedade e de dispensa de AIR.

> 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. 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.

Considerando que a proposta não implica em expressivo impacto financeiro ou orçamentário para os regulados , entende-se que a AIR pode ser dispensada com base no inciso III do art. 4º do Decreto nº 10.411, 2020.

8. Análise jurídica da Procuradoria Federal Especializada (PFE) junto ao ITI

PARECER n.00031/2024/PROFE/PFE-ITI/PGF/AGU

9. Alterações propostas

Minuta de resolução: Resolucao2xx6_descontinuidade_certificado_SSL.