INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI
DIRETORIA DE AUDITORIA, FISCALIZAÇÃO E NORMALIZAÇÃO
COORDENAÇÃO-GERAL DE NORMALIZAÇÃO E PESQUISA

Nota Técnica nº 004/2016 – CGNP/DAFN/ITI

Esclarecimento sobre o adiamento da revogação das políticas de assinatura que estava prevista para 28/11/2016.

O INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, Autarquia Federal, na qualidade de Autoridade Certificadora Raiz – AC Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, pelo conduto da Coordenação-Geral de Normalização e Pesquisa, subordinada à Diretoria de Auditoria, Fiscalização e Normalização, vem a público esclarecer que:

Esta nota técnica tem como objetivo informar sobre o adiamento da revogação das políticas de assinatura XAdES 2.2, das CAdES AD-RB, CAdES AD-RV, CAdES AD-RT e CAdES AD-RC, na versão 2.1, e a CAdES AD-RA na versão 2.2, que seria realizada em 28/11/2016, conforme descrito nas Notas Técnicas 1 e 3 da CGNP, publicadas em 01/06/2016 e 30/08/2016, respectivamente.

Em junho deste ano, quando essas políticas de assinatura foram disponibilizadas, ficou estabelecido um período de transitoriedade para que as aplicações legadas fossem ajustadas para o uso das novas versões de políticas de assinatura, bem como da nova organização das LPA. Assim, essas políticas de assinatura, tanto na codificação ASN.1 quanto na XML, seriam mantidas por 2 (dois) ciclos de LPA, contados a partir de 01/06/2016. Esse mesmo tempo foi aplicado à manutenção dos arquivos LPAv2, que seriam descontinuados na mesma data, ou seja, 28/11/2016.

No final do mês de outubro chegaram ao ITI solicitações de adiamento dessa data por pelo menos mais um ciclo. Essas solicitações foram apresentadas e discutidas nas reuniões do grupo permanente de trabalho para revisão do Padrão Brasileiro de Assinaturas Digitais, o GT PBAD, realizadas nos dias 04/10/2016 e 18/10/2016, onde chegou-se ao consenso que seria prudente adiar por mais um ciclo.

Esse adiamento atende à solicitação de setores envolvidos no contexto da certificação digital que ainda não estão plenamente aderentes às novas versões das políticas de assinatura ICP-Brasil lançadas em 01/06/2016, especialmente as restrições de uso de algoritmos SHA1.

Assim, a revogação das políticas de assinatura citadas e a descontinuidade dos arquivos identificados como LPAv2 ficou adiada para 26/02/2017, data em que se encerra o próximo ciclo de LPA.

Brasília, 28 de novembro de 2016

WILSON ROBERTO HIRATA:52049094949

Assinado de forma digital por WILSON ROBERTO HIRATA:52049094949
Dados: 2016.11.28 11:43:52 -02'00'

WILSON ROBERTO HIRATA
Coordenador-Geral de Normalização e Pesquisa

Nº GPROD: 04020.000356/2016-31