



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

Nota Técnica nº 002/2016 – CGNP/ITI

Esclarecimento sobre correções nas Políticas de Assinatura PAdES de Referências Completa (AD-RC) e de Arquivamento (AD-RA) e atualização na Lista de Políticas de Assinatura Aprovadas (LPA).

O INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, Autarquia Federal vinculada ao Ministério da Ciência, Tecnologia, Inovações e Comunicações, 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:

O Grupo de Trabalho Permanente de Revisão do Padrão Brasileiro de Assinaturas Digitais (GT PBAD), sob demanda do Comitê Gestor da ICP-Brasil, identificou falha nas Políticas de Assinatura (PA) do perfil PAdES, em sua versão textual, descrita no documento DOC-ICP-15.03, e na versão em código de máquina, disponibilizada no repositório da AC Raiz da ICP-Brasil.

As falhas afetaram as Políticas de Assinatura PAdES de Referências Completa (AD-RC) e de Arquivamento (AD-RA), notadamente na grafia das entradas CERT e CRL, do dicionário VRI, que estavam no plural quando deveriam estar no singular, em conformidade com a especificação ETSI TS 102 778-4, versão 1.1.2.

Ainda que essas falhas não comprometam e nem provoquem insegurança aos objetos assinados com essas políticas, entendeu-se ser necessário regularizar essa situação para manter coerência com a especificação do ETSI.

A regularização consistiu em revogar as políticas PAdES AD-RC e AD-RA, em suas versões 1.0, e gerar novas versões 1.1 dessas políticas. Para isto, nova LPA para o perfil PAdES foi gerada, contemplando as revogações e as novas versões dessas políticas e mantendo o ciclo de LPA para 30/08/2016.

Ainda que essas políticas de assinatura afetadas encontram-se atualmente expiradas, os objetos assinados durante o período de vigência, compreendido entre 01/06/2016 a 20/07/2016, devem ser considerados vigentes para efeito de verificação.

Brasília, 20 de julho de 2016

Wilson Roberto Hirata
Coordenação-Geral de Normalização e Pesquisa

Nº GPROD: