



MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
Instituto Nacional de Metrologia, Qualidade e Tecnologia - Inmetro
Dimel/CPC

Ofício Circular nº 2/2023/CPC/Dimel-Inmetro

INMETRO/SEI/NÚMERO DO PROTOCOLO
0052600.002527/2022-27

Duque de Caxias, 03 de março de 2023.

Para:
Postos Autorizados de Cronotacógrafos
Fabricantes de simuladores de pista dotados de banco de rolos - cronotacógrafo

Assunto: **Necessidade de revisão do protocolo de comunicação dos simuladores de pista**

Prezados Senhores,

1. Em 2022, a Coordenação-Geral de Tecnologia da Informação (Ctinf) do Inmetro identificou uma vulnerabilidade com o uso do protocolo SSL versão 3.0, utilizado por alguns simuladores de banco de rolos quando da comunicação com o Portal do Cronotacógrafo na transmissão dos ensaios, solicitando a alteração para o protocolo TLS versão 1.2 ou superior.
2. Frisa-se que essa condição é natural pela evolução tecnológica, e não significa problemas com os simuladores, mas apenas que o protocolo anterior, seguro quando da fabricação dos simuladores, pode admitir a falha conhecida como POODLE (*Padding Oracle On Downgraded Legacy Encryption*) que permite o conhecimento de mensagens criptografadas, identificado posteriormente e que pode fragilizar os sistemas do Inmetro.
3. Neste contexto, a Diretoria de Metrologia Legal (Dimel) emitiu o Ofício Circular nº 21/2022/Dimel-Inmetro para os fabricantes de simuladores de pista, comunicando a necessidade de atualização do protocolo e solicitando informações sobre a quantidade de simuladores nesta condição e as complexidades envolvidas para cada atualização.
4. Após os alinhamentos necessários e com o panorama definido, estamos certos de que em **06 de abril de 2023** possamos desabilitar as comunicações envolvendo o protocolo SSL 3.0, o que será imperceptível para os PACs em alguns simuladores.
5. Contudo, há uma quantidade razoável de simuladores que precisarão interromper seus serviços utilizando o simulador para a aplicação da correção. Diante disso, visando facilitar a logística e cientes de que essa atualização pode, inclusive, melhorar o tempo de resposta ao Portal de Cronotacógrafos, solicitamos o apoio dos PACs aos fabricantes, disponibilizando o acesso ao simulador quando for contatado, frisando que o tempo de atualização, em alguns casos, não ultrapassa os 5 minutos.
6. A expectativa é que todos os simuladores estejam atualizados na data prevista, de modo que simuladores irregulares não conseguirão transmitir os ensaios após 06/04/2023.
7. Cientes do apoio de todos os envolvidos no programa de verificação subsequente de cronotacógrafos, agradecemos a compreensão.

Atenciosamente,



DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO
ART. 6º, § 1º, DO [DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015](#) EM
03/03/2023, ÀS 18:16, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

EDUARDO RIBEIRO DE OLIVEIRA
Assistente

A autenticidade deste documento pode ser conferida no site

https://sei.inmetro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

informando o código verificador **1458091** e o código CRC **90A0813A**.



Av. Nossa Senhora das Graças, 50 - Bairro Xerém, Telefone: (21)2145-3228
CEP 25250-020/Duque de Caxias/RJ - www.inmetro.gov.br

Referência: Este Modelo integra os documentos da qualidade do Gabin/Presi e está referenciado à NIG-Gabin-030 - Rev. 012, publicada no Sidoq em Jun/2019.

sgqi@inmetro.gov.br