# NOTA PÚBLICA sobre el uso de criptografía en sistemas y dispositivos conectados a Internet

**ENGLISH VERSION | VERSÃO EM PORTUGUÊS**

EL COMITÉ GESTOR DE INTERNET EN BRASIL – CGI.br, en virtud de las atribuciones que le confiere el Decreto nº 4.829/2003, teniendo en vista la frecuente divulgación de iniciativas recientes que buscan crear acceso privilegiado a contenido de comunicaciones privadas en sistemas digitales, sea a través de mecanismos, procesos o herramientas que implementen vulnerabilidades o incluso que corrompan sistemas criptográficos; sea a través del desincentivo o “dificultaciones” del uso de criptografía, y

CONSIDERANDO

- Que el uso de criptografía fuerte es muy importante para que flujos de información se establezcan de forma segura y confiable en Internet, no solo para usuarios individuales, sino para empresas y órganos públicos;

- Que la protección de tales flujos se encuentra regulada en legislación

ordinaria (Ley 10.406 de 10 de enero de 2002 - Código Civil Brasileño; Ley 12.965 de 23 de abril de 2014 - Marco Civil de Internet, su Decreto regulador nr. 8.771/2016, art. 13, inc. IV; y Ley 13.709 de 14 de agosto de 2018 - LGPD, Ley General de Protección de Datos Personales, entre otras), y consta también de los “Principios para la Gobernanza y Uso de Internet” definidos por el CGI.br, en especial el principio de la libertad, privacidad y derechos humanos, según expreso en la Resolución **CGI.br/RES/2009/003/P**;

VIENE A PÚBLICO

- Reafirmar la importancia de garantizarse la posibilidad de implementación libre y adecuada de criptografía fuerte fin a fin, tanto para la protección del sigilo de datos y comunicaciones, como para el ejercicio de derechos previstos en la Constitución Federal y leyes infraconstitucionales;

- Reafirmar que una eventual implementación de mecanismos de acceso privilegiado a través de herramientas tales como “backdoors” o “llaves - maestras”, además de poder ser ineficaz ante intransponibilidades de orden técnico para la obtención del mensaje original, puede también representar riesgos mayores, al crear brechas de seguridad que se podrán explotar para fines maliciosos;

- Reafirmar que mecanismos criptográficos sólidos son fundamentales a la integridad y seguridad de sistemas digitales, al sigilo empresarial, como también a la garantía de la inimputabilidad de la red y de la funcionalidad, seguridad y estabilidad de Internet;

- Resaltar que una hipotética opción por mecanismos de criptografía vulnerables contrariaría a las mejores prácticas internacionales y afectaría severamente a la seguridad de los usuarios y de los emprendimientos en Internet, como también podría inhibir la innovación y el surgimiento de modelos de negocio.