RESOLUCIÓN
COMISIÓN TRANSITORIA PARA LA GESTIÓN DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA

Nro. 123-2016/CFE-INDECOPI

Lima, 09 de diciembre de 2016

Migración a algoritmo SHA-256

VISTO:

El Informe 017-2016-CFE de la Secretaría Técnica;

CONSIDERANDO:

Que, mediante su Resolución 073-2016/CFE-INDECOPI, de fecha 4 de agosto de 2016, y por las razones que en ella se exponen, en uso de las atribuciones acordadas al INDECOPI por el Reglamento de la Ley de Firmas y Certificados Digitales, la Comisión dispuso que a partir del 1 de enero de 2017 las entidades de certificación acreditadas o reconocidas por la Comisión utilizasen el algoritmo criptográfico SHA-256 en el proceso de generación de certificados digitales;

Que, del numeral (ii) del literal (b) del artículo 46 del citado Reglamento se desprende que los funcionarios públicos sólo pueden emplear certificados digitales generados por Entidades de Certificación del Estado Peruano acreditadas ante el INDECOPI, y a la fecha la única Entidad de Certificación del Estado Peruano que ha solicitado y obtenido la acreditación del INDECOPI es el Registro Nacional de Identificación y Estado Civil –RENIEC-;

Que, no obstante lo dispuesto en el literal (c) del artículo 48 del citado Reglamento, en el cual se establece que las Entidades de Certificación del Estado Peruano seguirán los lineamientos establecidos por la autoridad para la selección e implementación de los algoritmos criptográficos, el RENIEC ha informado a esta Comisión que por razones logísticas y presupuestarias no está en condiciones de generar certificados digitales con el algoritmo SHA-256 hasta el mes de abril de 2017;

Que, en dicho contexto, la aplicación estricta del plazo indicado en la Resolución 073-2016/CFE-INDECOPI colocaría a las entidades de la Administración Pública usuarias de los certificados digitales del RENIEC en una situación legalmente insostenible, pues los certificados digitales generados por su único proveedor reglamentariamente reconocido carecerían de efectos legales en la Infraestructura Oficial de Firma Electrónica, sin que, por otra parte, dichas entidades usuarias puedan recurrir a los demás proveedores acreditados por el INDECOPI;

Que, por tanto, con el objeto de no causar impases jurídicos a terceros que no son responsables de los hechos referidos en el tercer considerando, es necesario otorgar un plazo adicional para la migración del algoritmo SHA-1 al algoritmo SHA-256;

SE RESUELVE:

PRIMERO.- Las entidades de certificación pertenecientes a la Infraestructura Oficial de Firma Electrónica tienen plazo hasta el 30 de junio de 2017 para generar certificados digitales firmados con el algoritmo SHA-1. A partir del 1 de julio de 2017, dichas entidades de certificación quedarán obligadas a generar certificados digitales asociados al algoritmo SHA-256 u otro de mayor fortaleza criptográfica, sin necesidad de la emisión de una resolución administrativa adicional.

SEGUNDO.- Los certificados digitales generados con el algoritmo SHA-1 hasta el 30 de junio de 2017 sólo serán cancelados cuando se verifique alguna de las causales establecidas en el artículo 17 del Reglamento de la Ley de Firmas y Certificados Digitales.

TERCERO.- La adecuación del software acreditado y de los servicios acreditados de valor añadido que actualmente utilizan el algoritmo SHA-1 en el proceso de firmado de documentos electrónicos, los cuales también deberán migrar al algoritmo SHA-256 u otro de mayor fortaleza criptográfica, se verificará en la primera evaluación anual de seguimiento que corresponda realizar después del 30 de junio de 2017.

CUARTO.- Notifíquese la presente a los organismos acreditados y asimismo a las entidades usuarias que formularon consultas sobre la aplicación de la resolución 073-2016/CFE-INDECOPI.

Con la intervención de los señores miembros: Ítalo Laca Ramos, Pedro Astudillo Paredes y Fernando Casafranca Aguilar.

ÍTALO LACA RAMOS

PRESIDENTE DE LA COMISIÓN TRANSITORIA PARA LA GESTIÓN DE LA INFRAESTRUCTURA OFICIAL DE FIRMA ELECTRÓNICA