Al contestar por favor cite estos datos:
Radicado No.: *20162003001238 1*

Bogotá D.C., abril 11 de 2016

CIRCULAR 03 -2016

DE: DIRECCIÓN EJECUTIVA

ASUNTO: ADOPCIÓN ALGORITMO DE FIRMA SHA2 Y ALCANCE REQUISITO DE SUBCONTRATACIÓN CEA-4.1-10

DIRIGIDO A: ENTIDADES DE CERTIFICACIÒN DIGITAL - ECD
COORDINACION SECTORIAL DE ENTIDADES DE CERTIFICACION DIGITAL
EVALUADORES Y EXPERTOS TÉCNICOS ONAC
PÚBLICO INTERESADO

En el marco del programa de acreditación de Entidades de Certificación Digital – ECD y de los Criterios Específicos de Acreditación establecidos para dicho programa, en el documento CEA-4.1-10 Versión 01 de ONAC; se informa a las ECD acreditados, a las ECD solicitantes de acreditación, a los futuros usuarios del servicio de acreditación en este programa y al público interesado, que:

RESPECTO AL REQUISITO TÉCNICO ALGORITMO DE FIRMA SHA1

El numeral 10.11 del CEA-4.1-10 Versión 01, permite y requiere a las ECD mantener una evolución tecnológica no restrictiva frente a las mejoras emitidas en estándares y tecnologías en el entorno de PKI, ya sea en seguridad o en calidad, así:

"10.11Requisitos Técnicos
Los requisitos técnicos para el entorno de infraestructura de llave pública – PKI, deben mantener el principio de neutralidad tecnológica y vigencia. Los requisitos técnicos pierden vigencia una vez se establezca que está comprometida la seguridad o son declarados obsoletos, por lo que la ECD debe informar a ONAC y debe reemplazar por una nueva versión u otro estándar o componente, que no comprometa la seguridad y se encuentre vigente."
"13. ANEXOS TÉCNICOS Anexo A: Actividades 1,3, 4 y 6. Clasificadas como: Emisión de Certificados digitales (firmas digitales).
1. *Algoritmo de firma: (Función hash y RSA)*
   SHA1 con RSA Encryption no recomendado, se admite hasta la siguiente revisión por declaración de vulnerabilidad de SHA1."

Teniendo en cuenta lo anterior y considerando que OASIS PKI fórum, recomendó migrar el algoritmo SHA1 a SHA2 a partir del primero de enero de 2016; ONAC dispone:

1. A partir de la fecha, para todos las Entidades de Certificación Digital acreditadas, ECD en proceso de acreditación y nuevos solicitantes de acreditación en este programa, se requerirá como Algoritmo de firma (Función hash y RSA) SHA2 para segundo nivel de jerarquía o inferiores. Esta condición será verificada en el proceso de evaluación, tanto en etapa 1 como en etapa 2. Para quienes estando en proceso de evaluación de otorgamiento ya han superado dichas etapas, se requiere el envío inmediato de evidencias de la actualización, cuya verificación será adelantada en la evaluación complementaria correspondiente, en los plazos establecidos por las Reglas del Servicio de Acreditación; de haberse llevado a cabo ya la evaluación complementaría, se realizará evaluación extraordinaria documental cuyo resultado será indispensable para la decisión del Comité de Acreditación respecto al otorgamiento de la acreditación. Las demás ECD que pretendan acreditarse, deberán presentar junto con su solicitud, o complementar dicha solicitud si ya fue presentada, evidencia de la actualización, que será verificada durante la evaluación, en caso de que se pacte el servicio. El no cumplimiento inmediato de esta disposición implicará el no otorgamiento de la acreditación a las ECD solicitantes o en proceso de acreditación y el rechazo de solicitudes iniciales de acreditación.

2. La actualización a la nueva versión del Algoritmo de firma: (Función hash y RSA) SHA2, para la raíz o primer nivel de confianza, será exigible por ONAC a partir del 1° de octubre de 2016, fecha para la cual, tanto las ECD acreditadas, aquellas en proceso de acreditación o las nuevas solicitantes deberán demostrar el cumplimiento de esta disposición.

   - A partir del 1° de octubre de 2016, no se aceptarán solicitudes de acreditación para Entidades de Certificación Digital, si el solicitante no demuestra el cumplimiento de la adopción del Algoritmo de firma: (Función hash y RSA) SHA2 para la raíz o primer nivel de confianza y todos los niveles jerárquicos subsiguientes.
   - Las ECD acreditadas, estarán sujetas a evaluación extraordinaria para verificar el cumplimiento; frente al resultado de la evaluación deberá existir decisión del Comité de Acreditación antes del 1° de octubre de 2016, de lo contrario se procederá con la suspensión de la acreditación.
   - Para las ECD que a esa fecha no hayan iniciado el proceso de evaluación de otorgamiento, el cumplimiento requerido será verificado durante la etapa 1 y/o la etapa 2 de la evaluación programada.
   - Las ECD en proceso de acreditación que al 1° de octubre de 2016 ya hayan culminado la etapa 2 de la evaluación de otorgamiento, estarán sujetas a evaluación extraordinaria para verificar el cumplimiento de esta disposición, o podrán demostrar el mismo, en evaluación complementaria si esta fuera requerida.

   El no cumplimiento de este requerimiento en la fecha establecida, implicará la suspensión de la acreditación si ya ha sido otorgada; o la identificación de no conformidad frente a los requisitos de acreditación, y/o, el no otorgamiento de acreditación en caso de evaluaciones en curso.

RESPECTO AL REQUISITO "RECURSOS PARA LA SUBCONTRACIÒN"

En cuanto al numeral 10.4.2.1, del aparte "Recursos para la Subcontratación", del CEA-4.1-10 Versión 01, se aclara que, la ECD no podrá subcontratar la Autoridad de Registro (RA), ni la decisión acerca de la certificación.

Para que la confianza de calidad y seguridad de los servicios de certificación digital no se vea comprometida, la subcontratación que adelante la ECD en las demás materias, debe asegurar que sus contratistas no afecten el cumplimiento de la ECD frente a los requisitos de los criterios específicos de acreditación, en el contexto que la subcontratación involucre. Para esto, la ECD debe adoptar los controles que considere pertinentes, especialmente aquellos de la norma ISO/IEC 27001, que fueran aplicables en cada caso. Las actividades desarrolladas por estos subcontratistas podrán ser parte del alcance de la evaluación en el proceso de otorgamiento, mantenimiento o renovación de la acreditación de la ECD, en el contexto de los requisitos establecidos para cada actividad subcontratada.

Atentamente,

FRANCISCO JAVIER PIEDRAHÍTA DÍAZ
Director Ejecutivo

Revisó: Sandra Milena Medina
Director Técnico

Proyecto: Roberto Rodríguez Torres
Coordinador de Entidades de Certificación Digital