Esta nueva *Guía CCN-STIC 807* se encuentra en la parte pública del portal

Criptología de Empleo en el ENS, nueva Guía del Centro Criptológico Nacional

- **En la presente guía se actualizan los algoritmos criptográficos acreditados para el uso únicamente en el Esquema Nacional de Seguridad, ENS, cuando sus características y requerimientos se consideren necesarios.**

- **Se destaca la eliminación de las funciones resumen SHA-1 RIPMED-160 a partir de enero de 2017, así como la actualización de la longitud de clave para los algoritmos de clave pública.**

Madrid, 04 de mayo de 2015.- El CCN-CERT ha hecho pública la actualización de la **Guía CCN-STIC 807 Criptología de empleo en el Esquema Nacional de Seguridad** un completísimo documento en el que se presentan los algoritmos criptográficos que han sido acreditados para el uso únicamente en el ENS, cuando sus características y requerimientos se consideren necesarios. Las principal actualización de la guía es la eliminación de las funciones **resumen SHA-1y RIPMED-160 a partir de enero de 2017**. Las funciones resumen son utilizadas en los procesos de firma electrónica, derivación de claves, integridad de documentos, etc. Su seguridad se ha visto mermada con la aparición de nuevos algoritmos para su criptoanálisis y el incremento de la capacidad computacional. El CCN, en concordancia con las políticas aplicadas por empresas internacionales como Google, Mozilla, Microsoft, etc. y otros países, ha determinado que el algoritmo sha-1 no se encontrará acreditado a partir de enero del 2017.

"La seguridad debe adaptarse al estado del arte, las revisiones deben ser periódicas, adaptándose a las nuevas tecnologías y retos"

Además se han actualizado **las longitudes de clave** permitidas para los diferentes niveles de seguridad de los algoritmos de clave pública, aumentándose la longitud en concordancia con los avances computacionales.

En este sentido, es preciso recordar que dentro de la estructura del CCN se encuentra el **Organismo de Certificación (OC)** del Centro Criptológico Nacional que comprende a las entidades públicas o privadas que deseen ejercer como laboratorios de evaluación de la seguridad de las Tecnologías de la Información (TI) en el marco del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI). También incluye a las entidades públicas o privadas que sean fabricantes de productos o sistemas de TI que pretendan certificar la seguridad de sus productos en el marco del ENECSTI. Por esta razón los sistemas, productos y equipos evaluados y

Certificados por el CCN cumplen los requisitos de funcionalidad que tales productos afirman verificar en la declaración de seguridad.

La Guía, elaborada por el **Centro Criptológico Nacional**, recoge los algoritmos acreditados (cifrado simétrico, protocolos de acuerdo de clave, algoritmos asimétricos y funciones resumen) y los productos certificados. Asimismo, realiza una amplia exposición de las medidas de seguridad como los mecanismos de identificación y autenticación, la protección de la confidencialidad, autenticidad y de la integridad o el cifrado de la información.

Otras medidas de seguridad recogidas son la protección de claves critográficas, la firma electrónica o lo sellos de tiempo.

Sobre CCN-CERT, CERT Gubernamental Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del ENS.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, a sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

MÁS INFORMACIÓN

CCN-CERT
eventos@ccn-cert.cni.es
+34 670 29 20 05

Síguenos en
www.ccn-cert.cni.es/

@CCNCERT

http://youtu.be/5XxS9mZZfKs

COMUNICADO CCN-CERT

4 de mayo de 2015