# Boletín informativo del departamento de productos y tecnologías de seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

## Boletín CCN-PYTEC nº6 - 03/2018

## Productos STIC


### Primeras referencias al CPSTIC en Pliegos de Prescripciones Técnicas (03/2018).

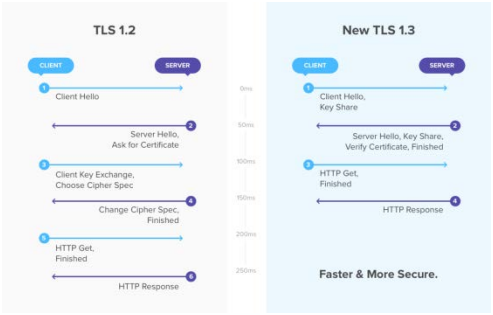
El Catálogo de Productos de Seguridad TIC (CPSTIC) del CCN se ha utilizado como referencia en el PPT que rige la celebración del acuerdo marco, a través del procedimiento especial de adopción de tipo, para el suministro de sistemas, equipos y software de comunicaciones (AM 10/2018). El CPSTIC se utiliza en este PPT para acreditar el cumplimiento de los requisitos funcionales de seguridad exigidos por el Esquema Nacional de Seguridad.

## Tecnologías para seguridad

### Proyecto para impulsar la soberanía europea en Systems on Chip (03/2018).

Dentro de la convocatoria de la Acción Preparatoria sobre Investigación en Defensa, lanzada por la EDA para este año 2018, se ha propuesto el proyecto "European high-performance, trustable, (re)configurable system-on-a-chip for defence applications". Este proyecto pretende impulsar la investigación en tecnologías SoC, empleadas en numerosos equipos para defensa, y particularmente en muchos productos de cifra. Actualmente este tipo de tecnologías son manufacturadas fuera de la UE, lo que implica un riesgo en cuanto a posibles vulnerabilidades de seguridad. Esta circunstancia en muchas ocasiones requiere la implementación de mecanismos de supervisión.

### Nuevo protocolos de red propuestos por la IETF (03/2018).




El CCN está estudiando los posibles implicaciones y usos de los nuevos protocolos de bajo nivel propuestos por la IETF (Internet Engineering Task Force). Dichos protocolos están orientados a mejorar la seguridad de la información, optimizar el rendimiento de los sistemas y acelerar las comunicaciones. Estos nuevos protocolos como HTTP/2, TLS 1.3, QUIC (Quick UDP Internet Connections) o DOH (DNS over HTTP) serán clave para aumentar el nivel de protección, la seguridad y la resiliencia de las redes de información nacionales, así como de los sistemas que manejen información sensible de la Administración y el Estado.

## Interoperabilidad

### Participación del CCN en el grupo de trabajo NATO KMISpec (03/2018).

Los días 4 y 5 de abril tendrá lugar la 5ª reunión del grupo de trabajo NATO KMISpec en las instalaciones de la NCIA en La Haya. El CCN participa de forma en activa en este grupo, cuyo objetivo es el desarrollo de una especificación para interoperabilidad de la gestión de claves de los cifradores empleados por OTAN. El principal objetivo de esta especificación es estandarizar el interfaz para facilitar la interoperabilidad en la gestión de claves entre equipos cripto e infraestructuras de gestión de claves, de forma que una única infraestructura permita dicha gestión incluso si estos equipos han sido fabricados por diferentes empresas o son operados por diferentes naciones. Durante la próxima reunión se revisará el borrador final para la versión 1.0 de la KM ISpec.

## Cifrado off-line

### Completada la implementación del CdC (03/2018).

Este mes de marzo se ha completado el diseño, desarrollo e implementación del Criptosoftware del CCN (CdC). El CdC es un software de cifrado offline que emplea claves asimétricas para garantizar la confidencialidad de la información y la identidad del emisor y los receptores. Este software ha sido diseñado tanto para ejecutarse de manera autónoma como para integrarse con los clientes de correo de la administración, Microsoft Outlook, pero también puede ser ejecutado a través de línea de comandos. En breve se comenzará la evaluación criptográfica del producto, con objeto de que cuando sea aprobado sustituya el uso de otros programas de cifrado offline asimétrico no aprobados de uso en la administración.

## Eventos

### Éxito de participación en los primeros desayunos tecnológicos CCN-PYTEC (03/2018).


El pasado 15 de marzo se celebró en la Escuela de Organización Industrial la primera edición de los desayunos tecnológicos CCN-PYTEC. En esta primera ocasión, el motivo del evento fue dar a conocer a la industria de seguridad y defensa el Catálogo de Productos STIC (CPSTIC) del CCN. La jornada tuvo una excelente acogida y contó con participantes procedentes de más de 80 empresas, que incluían tanto fabricantes como integradores de productos STIC en proyectos para la Administración. Está prevista la organización de un segundo desayuno tecnológico temático sobre el CPSTIC, pero esta vez enfocado al personal de la Administración.

## El CCN participa en el CSC(IA) de la UE y en el CaP4 de OTAN (03/2018).

Este mes de marzo el CCN ha participado en Bruselas en las reuniones del Grupo de Seguridad las TIC del Comité de Seguridad del Consejo de la Unión Europea (Council Security Committee (Information Assurance) - CSC(IA)) y del Panel para Aseguramiento de la Información y Ciberdefensa de la de OTAN (Information Assurance and Cyber Defence Capability Panel, CaP4). Estos dos comités son los responsables en UE y OTAN, respectivamente, de establecer los objetivos, las políticas, los planes y los programas en materia de seguridad de los sistemas CIS/TIC y en materia criptológica, de cara a contar con una capacidad CIS efectiva y segura en ambos ámbitos.

## El CCN participará en las primeras Jornadas CIS de las FAS (03/2018).

Durante los próximos días 4 y 5 de abril de 2018 se celebrarán en el CESEDEN las primeras Jornadas CIS de las Fuerzas Armadas. Este evento organizado por el Estado Mayor de la Defensa tiene como finalidad analizar el estado actual y establecer un Punto de Situación CIS Conjunto, en aras a impulsar y coordinar mejor los diferentes esfuerzos en curso para mejorar las capacidades CIS de las Fuerzas Armadas. Estas jornadas incluirán ponencias de la JCISFAS del EMAD, Ejército de Tierra, Armada, Ejército del Aire, MOPS, MCCD, CIFAS, UME y otros organismos. Por su parte, el CCN presentará los últimos desarrollos de productos criptográficos de interés para los CIS Tácticos.

## Contacto


| | |
|---|---|
| **Correo electrónico CCN-PYTEC** | ccn-pytec@cni.es |
| **Twitter** | **@CCNPYTEC** |
| **LinkedIn** | **https://www.linkedin.com/company/CCN-PYTEC** |