

CCN-PYTEC

centro criptológico nacional

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

Boletín CCN-PYTEC nº9 - 06/2018

Comunicaciones Móviles Seguras

Publicada la CCN-STIC-496 - Sistemas de Comunicaciones Móviles Seguras (06/2018).

En [esta guía](#), el CCN establece un conjunto de directrices para el diseño y despliegue de sistemas de comunicaciones móviles corporativos, así como para la revisión y adaptación de los ya existentes. La revisión y securización de los sistemas de telefonía móvil corporativos permitirá aumentar la seguridad de la información en cualquier organización, ya que es habitual que este subsistema sea uno de los grandes "agujeros" en la organización. El objetivo es dotar a los sistemas de mayor seguridad, tanto para las comunicaciones establecidas con los dispositivos, como para la información almacenada en los mismos.



Comunicaciones Tácticas Seguras

El CCN trata la evaluación de equipos SDR durante su visita a Eurosatory (06/2018).



El CCN ha asistido a la última edición de la feria de defensa Eurosatory, celebrada en París entre los días 11 y 15 de junio. La representación del CCN formó parte de la delegación española procedente de la Dirección General de Armamento y Material (DGAM) del MINISDEF. Durante las reuniones con los diferentes fabricantes de radios militares definidas por software (SDR) presentes en la feria, el CCN expuso su enfoque para la evaluación de seguridad de este tipo de productos criptográficos. En este sentido cabe destacar que los equipos que se adquieran en el programa del Sistema Conjunto de Radio Táctica, deberán someterse a las evaluaciones requeridas por el CCN para la posterior aprobación para el manejo de información clasificada nacional.

Cifrado IP

Aprobada la nueva versión del EP430TX (06/2018).

La nueva versión 1.04 del cifrador IP EP430TX (SECRETO NACIONAL) ha sido aprobada nacionalmente por el CCN de forma interina. Esta actualización del equipo incorpora nuevas funcionalidades y será proporcionada por el fabricante EPICOM.



Superadas las pruebas de aceptación del MAVIP RESTRICTED (06/2018).



Durante este mes de junio, se han llevado a cabo las pruebas de aceptación del prototipo del cifrador IP de muy alta velocidad, correspondientes al expediente de I+D MAVIP-R del programa CIFIPEVOL de la DGAM. Este prototipo, con un “throughput” agregado de hasta 17 Gbit/s a nivel IP y de hasta 35 Gbit/s a nivel MACSec, es la base de un producto indicado para la protección del Núcleo Protegido de Red de la futura red I3D del Ministerio de Defensa.

Interoperabilidad

El cifrador táctico CIFPECOM en CWIX 2018 (06/2018).



La empresa TecnoBIT y el CCN han participado los días 21, 22, 25 y 26 de junio en el ejercicio CWIX 2018 que tuvo lugar en Bydgoszcz (Polonia). Durante el ejercicio se validó la implementación SCIP multipunto y NINE tactical radio profile del cifrador táctico TZ-1001, evolución del Cifrador Personal del Combatiente (CIFPECOM). Por una parte, se llevaron a cabo pruebas de interoperabilidad con cifradores SCIP y NINE de otras naciones. Además, el CIFPECOM también se probó sobre la red radio de coalición conformada por equipos SDR (“software defined radio”) de Thales, Leonardo y Bittium, los cuales interoperaban entre sí mediante la forma de onda ESSOR HDR WF. Las pruebas fueron exitosas y particularmente llamó la atención la solución SCIP multipunto como voz “Push-To-Talk” sobre la ESSOR HDR WF.

Participación nacional en los grupos de trabajo SCIP y NINE (06/2018).

Durante la semana del 18 al 25 de junio, se celebró en La Haya la primera reunión de los grupos de trabajo SCIP y NINE del CIS3 C&I Partnership. Estos grupos tienen por objeto el desarrollo e implantación de los protocolos de interoperabilidad a nivel de aplicación (SCIP) y a nivel de red (NINE) en la OTAN, y están integrados tanto por las NCSAs adheridas al Acuerdo como por las empresas que están desarrollando equipos que cumplen con estos estándares (EPICOM y TECNOBIT en España). En este foro el CCN ha expuesto su estrategia para el desarrollo e implantación de estos sistemas en los escenarios nacionales, en línea con la estrategia de la Alianza para la implantación de sistemas interoperables en los ámbitos estratégico y operativo.



Productos STIC

Novedades en el listado de productos aprobados (06/2018).

Se han incluido dos nuevos productos aprobados, pertenecientes a la familia de pasarelas de intercambio seguro de información, en el Listado de productos aprobados del Catálogo de productos de seguridad TIC (CPSTIC):

PSTfile

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile, automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.



PSTmail

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways, que permite el intercambio controlado de correo electrónico entre dominios de seguridad. Además, posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura; y soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Junto a la aprobación de los productos anteriores se ha publicado la correspondiente [guía CCN-STIC-1401 "Configuración segura de pasarelas de AUTEK INGENIERIA"](#), que describe el procedimiento de empleo tanto para sistemas afectados por el Esquema Nacional de Seguridad (ENS), como por sistemas que manejen información nacional clasificada.



Eventos

El CCN ha participado en el Crypto-CaT de la OTAN (06/2018).

Dentro del marco Grupo de Capacidades Criptográficas (CRYPTO CaT) de la OTAN, y como resultado de los procesos de criptomodernización de la Alianza, se está procediendo a la actualización de la normativa de seguridad en varios ámbitos. Algunas de las directivas más destacadas que están siendo revisadas con:



- Seguridad en las Emisiones AC/322-D(2007)0036.
- Seguridad en la Transmisión AC/322-D/0049.
- Control y custodia del material criptográfico de la OTAN - SDIP293/1.

Cuando se aprueben oficialmente las nuevas versiones, se procederá a su remisión a los órganos implicados nacionalmente para su aplicación.

Contacto

Correo electrónico CCN-PYTEC

Twitter

LinkedIn

ccn-pytec@cni.es

@CCNPYTEC

<https://www.linkedin.com/company/CCN-PYTEC>