

# 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 nº18 - 07/2019

#### Comunicaciones Tácticas Seguras

##### Primera prueba de concepto de LTE seguro desplegable (07/2019).

El 11 de julio se llevó a cabo la primera prueba de concepto de tecnología LTE para entornos desplegables y securizada con soluciones de cifra aprobadas por el CCN para procesar información clasificada. La prueba se llevó a cabo con la celda LTE-TPN400 de la empresa CENTUM. LTE-TPN400 es un equipo radio ligero y robusto capaz de crear una red privada de comunicaciones LTE plenamente funcional desde cualquier tipo de vehículo. Ha sido diseñada bajo estándares aeronáuticos, lo que le permite operar con fiabilidad en los escenarios más duros y exigentes. Se trata de un dispositivo altamente escalable y configurable que puede trabajar en cualquier banda LTE desplegada mundialmente.



Sobre esta infraestructura de comunicaciones se empleó con éxito la suite de seguridad conformada por el teléfono móvil ruggedizado Bittium Tough Mobile C y la aplicación ComsecAdmin+ de Indra para comunicaciones seguras de voz, datos y video. Tanto el Bittium Tough Mobile C como la app ComsecAdmin+ están incluidas en el Catálogo de Productos STIC en la categoría de Comunicaciones Tácticas Seguras.

Cabe destacar que la arquitectura de seguridad adoptada en estas pruebas con la celda LTE-TPN400 para entornos desplegables, es similar a la que se ha venido empleando durante los últimos meses en las pruebas de Wi-Fi seguro llevadas a cabo por la JCISAT del Ejército de Tierra y el CCN. Durante los próximos meses está prevista la realización de pruebas de prestaciones, tanto en laboratorio como en campo, con esta celda LTE y también con celdas de otros fabricantes.

#### Intercambio seguro de información

##### PST-Diode de AUTEK, empleado con éxito en CWIX 2019 (06/2019).

El diodo UDP de AUTEK (PST-Diode) fue empleado con éxito en el ejercicio CWIX de la OTAN entre los días 10 y 27 de junio de 2019. Este dispositivo de protección de perímetro fue usado para facilitar el



intercambio seguro de información entre la red CWIX sin clasificar y la red CWIX clasificada, conocida como “pink network”. PST-Diode permitió los flujos de datos UDP de la red de menor nivel a la de mayor nivel; en concreto, se distribuyeron datos de posiciones de unidades tácticas empleando los protocolos FFI, VMF y JDSS, los cuales eran generados por sistemas reales de dotación en Fuerzas Armadas tales como VLAD, VERT o BMS. La participación de AUTEK en CWIX 2019, esponsorizada por la Jefatura CIS y Asistencia Técnica (JCISAT) del Ejército de Tierra, supuso una oportunidad inmejorable para el empleo de PSTdiode en un entorno operativo relevante.

## Productos STIC

### Symantec Endpoint Protection Mobile cualificado en la familia “anti-virus / EPP (Endpoint Protection Platform)” para ENS categoría media (06/2019).

El producto Symantec Endpoint Protection Mobile (SEP Mobile) se ha incluido en el Catálogo de Productos de Seguridad TIC como cualificado para ENS media.



SEP Mobile es una solución de defensa de entornos móviles multiplataforma, cuyo objetivo es detectar amenazas tanto existentes como desconocidas.

### FortiMail, cualificado en la familia “anti-spam” para ENS categoría alta (06/2019).

Los siguientes productos del fabricante Fortinet se ha incluido en la familia “anti-spam” en el Catálogo de Productos de Seguridad TIC como cualificado para ENS Alta:



FortiMail es un sistema de seguridad de correo electrónico que proporciona una protección multicapa contra spam, virus, gusanos y spyware. El motor de filtrado empleado en FortiMail bloquea el spam y el malware antes de que pueda afectar a las redes y usuarios.



### Productos aprobados en las familias de “switches” para su uso en sistemas que manejan información clasificada (06/2019).

Se han incluido 12 productos en el Catálogo de Productos de Seguridad TIC, en la familia de “switches”, como aprobados para su uso en sistemas que manejan información clasificada. Los productos incluidos en el CPSTIC pertenecen a los siguientes fabricantes:



## Rubrik, aprobado en la familia de “copias de seguridad” para su uso en sistemas que manejan información clasificada (06/2019).

El fabricante Rubrik ha obtenido la aprobación de los siguientes productos para su inclusión en la familia de “copias de seguridad” del Catálogo de Productos de Seguridad TIC:



Rubrik ofrece disponibilidad instantánea de la información para recuperación ante desastre, ataque “ransomware” o pruebas de desarrollo. Se trata de una solución definida por software que permite una operación sencilla, construida con arquitectura “scale-out”, basada en sistemas distribuidos, que reparten de forma inteligente y autónoma los datos, metadatos y tareas entre todos los nodos y miembros del clúster, permitiendo realizar búsquedas globales, indexadas y predictivas “google-like”.

Al tratarse de un producto que maneja información clasificada se limitan ciertas opciones de configuración –véase la guía CCN-STIC -1606 Procedimiento de Empleo Seguro Rubrik- como la interconexión con un servicio en la nube.

## Primeros productos aprobados en la nueva categoría de Comunicaciones Tácticas Seguras del CPSTIC (06/2019).

En la revisión del Catálogo de Productos STIC del CCN (CCN-STIC-105) de junio de 2019, se han incluido los primeros productos aprobados para procesar información clasificada en la nueva categoría del CPSTIC denominada “Comunicaciones Tácticas Seguras”. En la familia de plataformas y dispositivos tácticos confiables se han incluido el teléfono móvil ruggedizado Bittium Tough Mobile C y la tablet ruggedizada GETAC F110G4. Por su parte, en la familia de soluciones para protección de las comunicaciones tácticas se ha incluido la aplicación para comunicaciones seguras ComsecAdmin+. A medida que se vayan completando las necesarias evaluaciones de seguridad que están en curso, se irán incorporando nuevos productos en esta categoría del CPSTIC.



### Eventos

## Éxito de asistencia al I Encuentro del Esquema Nacional de Seguridad (06/2019).

El martes 18 de Junio tuvo lugar el I Encuentro del Esquema Nacional de Seguridad en el Auditorio de la Fábrica Nacional de la Moneda y Timbre en Madrid. El evento, organizado por el Centro Criptológico Nacional, contó con la colaboración del Ministerio de Política Territorial y Función Pública (Secretaría General de Administración Digital) y de la Fundación Círculo de Tecnologías para la Defensa y la Seguridad. En este Encuentro ENS se dieron cita más de 350 responsables de

seguridad, tanto del sector público como privado, con el objeto de hacer balance del desarrollo e implantación del ENS y, sobre todo, de los nuevos retos que se plantean a partir de ahora.

Cabe destacar que el Jefe del Departamento de Productos y Tecnologías del CCN ofreció una presentación sobre el trabajo realizado por este organismo para establecer los requisitos funcionales de seguridad mínimos exigibles a cada taxonomía de productos de seguridad TIC para su empleo en la Administración. Este trabajo está recogido en la CCN-STIC-140 y sirve como base para el desarrollo del Catálogo de Productos de Seguridad TIC (CCN-STIC-105).

## Segunda Reunión de los grupos de trabajo SCIP y NINE de la iniciativa CIS3 Partnership

La semana del 24 al 28 de junio, el CCN ha participado en la Segunda Reunión de los Grupos de trabajo para el desarrollo e implantación de los estándares de la OTAN para la protección de voz segura SCIP (*Secure Communications Interoperability Protocol*) y protección de transmisiones IP NINE (*Network and Information Infrastructure IP Network Encryption*). Dentro de este marco, y en paralelo a las sesiones principales, se reunieron los *focus group* que están desarrollando los perfiles específicos de radio de ambos estándares y de interoperabilidad con el estandar de voz americano, TSVICIS.

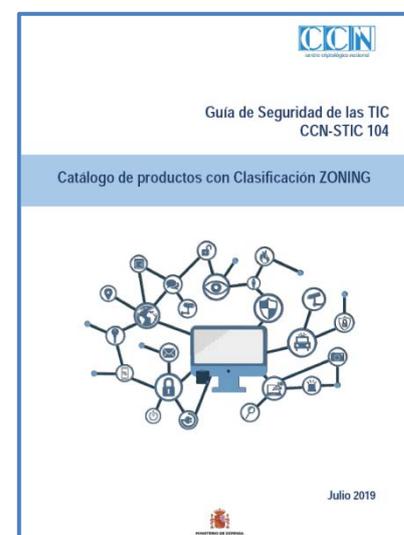


Durante las sesiones que se celebraron en la Haya (Países Bajos), el CCN presentó la evolución de la estrategia nacional para el desarrollo de productos nacionales basados en estos estándares, y expuso los resultados obtenidos en el ejercicio CWIX'19 por los productos desarrollados por empresas nacionales que implementan los estándares SCIP y NINE, además del diodo nacional que se utilizó como dispositivo de intercambio seguro de información en la red del ejercicio.

## EMSEC

### Actualización de la guía CCN-STIC-104 (07/2019).

Este mes de julio se ha publicado una nueva versión actualizada de la guía CCN-STIC-104 "Catálogo de Productos con clasificación ZONING" que incluye los últimos equipos y sistemas evaluados por el laboratorio TEMPEST del CCN. La consulta de este catálogo permite obtener una orientación en cuanto a la selección de equipamiento informático que pueda cumplir con una determinada clasificación ZONING. Es de aplicación para equipos que manejen información clasificada NATO CONFIDENTIAL/EU CONFIDENTIAL/CONFIDENCIAL, o superior, y vayan a ser instalados en locales con clasificación ZONING de ZONA 1 o superior. La clasificación mostrada en esta guía es sólo orientativa y no exime de la necesidad de evaluar los equipos, especialmente si la información que se va a procesar es NATO SECRET/EU SECRET/ RESERVADO o superior.



## Contacto

Correo electrónico CCN-PYTEC

[ccn-pytec@cni.es](mailto:ccn-pytec@cni.es)

Twitter

@CCNPYTEC

LinkedIn

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

Catálogo CPSTIC

[Enlace web](#)

