Boletín informativo del Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PYTEC).

Boletín CCN-PYTEC nº27 - 11/2020

Comunicaciones Tácticas Seguras

El CCN participa en unas pruebas organizadas por la Armada sobre 4G/LTE seguro en el BAM P-46 "Furor" (11/2020).

Durante los días 4 y 5 de noviembre la **Armada española y la empresa Navantia Sistemas** organizaron unas pruebas en el **Buque de Acción Marítima P-46 "Furor"** para probar tres celdas 4G/LTE facilitadas por la UTE TELEFÓNICA-AICOX, por la empresa GALICOM y por la empresa CENTUM. El objetivo de la Armada durante estas pruebas era evaluar la idoneidad de la tecnología LTE para dar soporte a ciertas operaciones en las que se requiere contar con un enlace estable de video en tiempo real.

Por su parte, el CCN participó en dichas pruebas aportando la solución **Comsec Admin Plus de la empresa Indra**, aprobada para DIFUSIÓN LIMITADA y NATO RESTRICTED, para el establecimiento de **comunicaciones seguras de voz y videoconferencia** entre terminales LTE de diferentes bandas (se probó en banda 28 y banda 31), así como con dispositivos Windows.

Las pruebas realizadas con Comsec Admin Plus mostraron que esta solución se adapta perfectamente a las necesidades de la Armada en este escenario, con independencia de la celda 4G/LTE y de los terminales móviles empleados en cada caso.

El cifrador táctico TZ-1001 v2.4 (proyecto CIFPECOM) aprobado para la protección de información clasificada nacional (11/2020).

El **cifrador táctico TZ-1001 v2.4 de la empresa TECNOBIT (Grupo Oesía)** ha sido aprobado en sus configuraciones C y R para la protección de **información clasificada nacional CONFIDENCIAL** y **DIFUSIÓN LIMITADA**, respectivamente. Este cifrador, cuyo desarrollo se inició en el proyecto CIFPECOM de la DGAM del Ministerio de Defensa Español, está concebido para la protección de las comunicaciones sobre redes de bajo ancho de banda y sin estabilidad de enlace garantizada (p.ej. Red Radio de Combate, "SATCOM on the move", etc.).

Actualmente este cifrador está en **proceso de integración con** diversos sistemas CIS tácticos de Fuerzas Armadas, tales como **el Gestor de Comunicaciones del Ejército de Tierra (GESCOMET)**, para dotarlos de una capacidad de cifrado de datos IP y de voz táctica "push to talk".

Novedades en el Catálogo de Productos STIC

"Herramientas para desarrollo de productos de seguridad", nueva categoría en el CPSTIC (11/2020).

Con el objetivo de facilitar el desarrollo y las evaluaciones de seguridad de los productos STIC, se ha creado una **nueva categoría dentro del CPSTIC que recoge una serie de herramientas de referencia validadas por el CCN**. Las dos primeras herramientas incluidas en la categoría son la librería cripto BOTAN-CCN y el IP Core TRNG-P200.

El TRNG-P200 de la empresa BERTEN es un Generador de Números Aleatorios Verdaderos (TRNG, True Random Number Generator) que se puede implementar en cualquier diseño criptográfico basado en FPGA, SoC o ASIC. Sus características lo hacen adecuado para su empleo en productos cripto de nivel alto de seguridad.

Por su parte, la librería cripto BOTAN-CCN implementa los mecanismos criptográficos aceptados por el CCN. Esta librería va a ser la **herramienta de referencia para la evaluación criptográfica de productos STIC. Además, es posible su uso en el desarrollo de productos de seguridad**. Incluye código fuente y binarios compatibles con sistemas Windows y Linux. Incluye generadores de ruido y tests de todos los mecanismos implementados.

Actualizada la guía CCN-STIC-106 para la inclusión de SERVICIOS CUALIFICADOS en el CPSTIC (11/2020).

La guía CCN-STIC-106 detalla, por primera vez**, el procedimiento y las evaluaciones requeridas a un servicio de seguridad TIC para ser incluido en el Catálogo de Productos y Servicios STIC (CPSTIC).**

Además de recoger este proceso, en el documento se detallan los motivos por los cuales un producto o servicio podría ser excluido del CPSTIC, así como las certificaciones y evaluaciones requeridas para que un producto o servicio de seguridad sea considerado cualificado.

La guía incluye un total de **tres anexos**:

- **Anexo A.** Solicitud de inclusión de un producto o servicio de seguridad en el CPSTIC.
- **Anexo B.** Declaración responsable de capacidad de suministro de logs.
- **Anexo C.** Certificado de cualificación y distintivo de producto o servicio cualificado.
  - C.1. Certificado de cualificación de producto.
  - C.2. Distintivo de producto cualificado.
  - C.3. Certificado de cualificación de servicio.
  - C.4. Distintivo de servicio cualificado.

CCN-PYTEC está actualmente trabajando en la elaboración de **dos nuevos anexos**, que serán publicados próximamente:

- **Anexo D.** Evaluaciones STIC Complementarias, de acuerdo a la metodología LINCE.
- **Anexo E.** Cualificación de series de productos.

SAMSUNG ha cualificado en la familia de 'Dispositivos móviles', para categoría ALTA, dispositivos con Android 10: Galaxy S20, Galaxy A51, Galaxy Tab S6 y Galaxy XCover Pro (11/2020).

La familia de dispositivos de la gama **Galaxy S20 + 5G (SM-G986B), S20 5G (SM-G981B), S20 Ultra 5G (SM-G988B), S20+ 4G (SM-G985F), S20 4G (SM-G980F)** son teléfonos móviles basados en Android que incorporan la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

Galaxy A51 (SM-A515F) es un teléfono móvil basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA: ALTA

Dispositivos Móviles

Samsung Galaxy Tab S6 (SM-T860, SM-T865) es una tableta empresarial basada en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo *hardware*, protección robusta a los datos en reposo y datos en tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA: ALTA

Dispositivos Móviles

Galaxy XCover Pro (SM-G715FN) es un teléfono móvil rugerizado basado en Android que incorpora la Plataforma Samsung Knox, ofreciendo mecanismos de protección de integridad con respaldo Hardware, protección robusta a los Datos en Reposo y Datos en Tránsito, así como el control avanzado y monitoreo del dispositivo de manera transparente y productiva para el usuario de la organización.

ens Esquema Nacional de Seguridad — ALTA / MEDIA / BÁSICA: ALTA

Dispositivos Móviles

Publicada la guía CCN-STIC-1204 "Procedimiento de empleo seguro ESET Endpoint Security 7" (11/2020).

El CCN ha publicado la guía "CCN-STIC-1204 Procedimiento de Empleo Seguro ESET España Endpoint Security 7", para sistemas ENS de categoría MEDIA.

Eventos

El ITEFI-CSIC y CCN-PYTEC convocan la III edición del premio "Tengo un proyecto" (11/2020)

El ITEFI-CSIC y CCN-PYTEC convocan la III edición del premio "Tengo un proyecto" al mejor Trabajo de Fin de Grado o Proyecto Fin de Master en Criptología, con una dotación en metálico de 1.000€.

Contacto

Correo electrónico CCN-PYTEC	**ccn-pytec@cni.es**
Twitter	**@CCNPYTEC**
LinkedIn	**https://www.linkedin.com/company/CCN-PYTEC**
Catálogo CPSTIC	**https://ccn.cni.es/cpstic**
Youtube	**youtube.com/channel/UCuSR7guHgx5kgoj6kafOF1Q**

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

CCN-PYTEC
Praeventio sit vincere