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

Boletín CCN-PYTEC nº12 - 11/2018

Interoperabilidad

El CCN asiste al Comité Director del programa CIS3 C&I Partnership (10/2018).

El CCN participó, entre los días 29 y 31 de octubre, en las reuniones del Comité Director del programa CIS3 C&I Partnership, así como en los paneles de los paquetes de trabajo para el mantenimiento y evolución de los estándares SCIP y NINE. Este programa internacional gestionado por la NCIA cuenta con la participación de Alemania, Canadá, España, Estados Unidos, Francia, Italia, Noruega, Países Bajos, Polonia, Reino Unido, República Checa y Turquia; además, Eslovenia y Finlandia asisten provisionalmente a las reuniones como observadores. Durante estas reuniones, que tuvieron lugar en las nuevas instalaciones del Cuartel General de la OTAN en Bruselas, se trataron las alternativas para dar continuidad al programa hasta el año 2020 y en adelante. Además, el CCN presento los entornos de pruebas SCIP y NINE propuestos para el ejercicio CWIX 2019.

Comunicaciones Tácticas Seguras

Pruebas del CIFPECOM junto con terminales SECOMSAT-D (10/2018).

El cifrador táctico CIFPECOM fue empleado con éxito en las pruebas que se llevaron a cabo con terminales “manpack” SECOMSAT Desplegable (SECOMSAT-D) entre los días 8 y 11 de octubre de 2018 en Los Alcázares (Murcia). Durante estas pruebas, organizadas por la Oficina de Programa SECOMSAT-D de la Dirección General de Armamento y Material del MINISDEF (DGAM/SDGGESPRO), se evaluaron los terminales “manpack” de las empresas Indra e Inster. En ambos casos se empleó el CIFPECOM, de la empresa Tecnobit, como dispositivo de cifra sobre la red i-Direct en una configuración de doble salto satélite (pasando por la estación de anclaje en Bermeja).

Comunicaciones Móviles Seguras

Los teléfonos móviles, blanco de los ciberataques (10/2018).

Durante las jornadas de ciberseguridad, organizadas por la Asociación para el Progreso de la Dirección el pasado 3 de octubre en Málaga, el Subdirector General del CCN indicó que los usuarios de teléfonos móviles que hagan uso de los servicios de almacenamiento e información en la nube sin tomar las medidas de protección adecuadas, corren el riesgo de ser vícitimas de un ciberataque. En ese sentido, Luis Jiménez destacó que las vulnerabilidades del sistema operativo suelen ser el vector de ataque empleado. Por ello, es muy importante comprobar la fecha del último parche de seguridad de nuestros móviles y mantenerlos actualizados.

En el caso de uso corporativo, el CCN propone en la guía CCN-STIC-496 un conjunto de directrices para el diseño y despliegue de sistemas de comunicaciones móviles, así como para la revisión y adaptación de los ya existentes. Haciendo uso de los dispositivos adecuados del Catálogo CPSTIC (cualificados o aprobados según el tipo de información manejada) y las configuraciones recomendadas disminuye la probabilidad de ser victima de un ciberataque.

EMSEC

El CCN asiste al Simposio TEMPEST, convocado por el Consejo de la UE (10/2018).

El CCN asistió el pasado mes de octubre al tercer Simposio TEMPEST Europeo, impulsado por el Consejo de la UE y organizado en esta edición por la Autoridad TEMPEST Sueca en la Base Naval de Karlskrona.

En estas reuniones las autoridades nacionales, laboratorios y empresas fabricantes discuten abiertamente sobre el desarrollo de normativa y ponen en común sus procedimientos e inquietudes colaborando en la formación técnica de la Comunidad TEMPEST, así como en la definición de los requisitos exigibles a equipos, instalaciones y plataformas a fin de mitigar el riesgo de emanaciones comprometedoras.

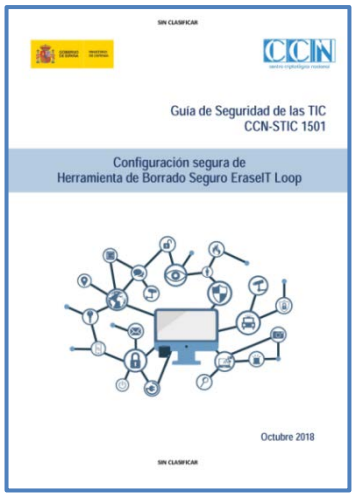
Productos STIC

Novedades en el Catálogo de Productos STIC (10/2018).

En la publicación del mes de octubre del Catálogo de Productos de Seguridad TIC (CPSTIC), publicado en la guía CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación, se han incluido tres nuevos productos correspondientes a las siguientes familias del listado de productos:

- Herramientas antivirus / EPP.
- Herramientas para comunicaciones móviles seguras.

Nueva guía de configuración de la herramienta de borrado seguro EraseIT Loop (11/2018).



La Guía CCN-STIC-1501 recoge el procedimiento de empleo seguro de la herramienta EraseIT Loop, la cual está incluida en el Catálogo de Productos de Seguridad TIC (CPSTIC) como herramienta de borrado seguro en sistemas afectados por el Esquema Nacional de Seguridad hasta categoría Alta.

EraseIT Loop es una herramienta software que borra de forma segura, definitiva e irreversible todos los datos de los dispositivos de almacenamiento de un equipo informático, incluido el disco de sistema, lo que permite su reciclaje o reutilización de manera segura. El proceso de borrado se realiza mediante sobrescritura de datos.

Eventos

CCN-PYTEC estará presente en las XII Jornadas STIC CCN-CERT (11/2018).

El próximo 12 Diciembre, en las XII Jornadas STIC CCN-CERT "Ciberseguridad, hacia una respuesta y disuasión efectiva", el Departamento de Productos y Tecnologías del CCN impartirá la ponencia "*CCN-PYTEC y CPSTIC: Generando confianza en la Administración*", dentro del módulo de Prevención en Ciberseguridad. El evento tendrán lugar los días 12 y 13 de diciembre en Kinépolis de Madrid (Ciudad de la Imagen). La solicitud de inscripción debe realizarse a través del formulario de la web de las Jornadas. El evento es gratuito, aunque el acceso a las Jornadas está sujeto a la validación de la solicitud por parte de la organización.

Contacto

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