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

Boletín CCN-PYTEC nº15 - 03/2019

Especial por el 15º aniversario del Centro Criptológico Nacional

Quince años de CCN-PYTEC (03/2019).

El pasado 12 de marzo el Centro Criptológico Nacional celebró su 15º aniversario. Durante estos quince años, el CCN ha trabajado para garantizar un ciberespacio más seguro y confiable. En particular, el desarrollo, la evaluación y la certificación de productos STIC han sido piezas clave dentro de las actividades de prevención y protección frente a los ciberataques. Precisamente ese ha sido el principal cometido del Departamento de Productos y Tecnologías, PYTEC, que durante estos quince años ha puesto a disposición de la Administración productos y soluciones para el adecuado procesamiento y protección de la información nacional sensible, con especial atención a la información clasificada. Uno de los resultados de este trabajo ha sido el Catálogo de Productos STIC del CCN (CCN-STIC-105), que recoge los productos cualificados para uso en los sistemas de la Administración española afectados por el Esquema Nacional de Seguridad, asi como los Productos STIC aprobados para procesar información nacional clasificada. Además, cabe destacar que algunos de estos productos STIC nacionales gozan de reconocimiento internacional al estar aprobados para su uso en OTAN y UE.

El Departemento PYTEC del CCN, en colaboración con otros organismos, con los laboratorios del ENECSTIC y con la industria nacional del sector, continuará orientando sus esfuerzos, energías y recursos para seguir proporcionando productos STIC que cubran las necesidades de la Administración y cuya seguridad haya sido contrastada nacionalmente. Esa es la mejor contribución posible para fortalecer la ciberseguridad en España.

Quince años proporcionando productos de cifra soberanos (03/2019).

Durante estos quince años, el CCN-PYTEC ha impulsado el desarrollo, la evaluación y la aprobación de productos de cifra nacionales para proteger la información nacional clasificada del más alto nivel de seguridad. En este sentido, seguir contando con una industria nacional especializada es un objetivo estratégico puesto que la soberanía de las comunicaciones nacionales más críticas está en juego. Además, los esfuerzos del CCN-PYTEC y de la industria nacional también han conseguido un reconocimiento internacional, destacando dos hechos muy significativos:

- El 2 de mayo de 2013, el cifrador IP EP430GN fue aprobado por el NATO Military Committee (NAMILCOM) para la protección de información hasta grado NATO SECRET, tras haber superado la evaluaciones de CCN y SECAN (laboratorio de evaluación OTAN). A partir de ese momento, España adquirió el estatus de nación productora de equipos de cifra (CPN, Crypto Producing Nation) en OTAN.

- El 11 de octubre 2017, el teléfono móvil seguro Färist Mobile fue aprobado por la Unión Europea para la protección de información clasificada hasta grado UE RESTRICTED, tras haber superado las evaluaciones del CCN y de la autoridad nacional para la seguridad de los sistemas CIS de Suecia. De esta forma, España fue la primera nación no AQUA (grupo de naciones europeas que realizan segundas evaluaciones) que obtuvo una aprobación de la Unión Europea para un producto nacional.

El próximo gran reto de CCN-PYTEC es la obtención de la aprobación de la Unión Europea del cifrador IP EP430GU para la protección de información clasificada hasta grado EU SECRET. Para ello, este cifrador se está sometiendo a proceso de segunda evaluación (“Second Party Evaluation”) por parte de la Agencia Nacional de la Seguridad de los Sistemas de Información francesa (ANSSI). Esa aprobación supondrá el cumplimiento de uno de los requisitos clave para que España se convierta en nación AQUA.

Organismo de Certificación del CCN, generando confianza en la Administración (03/2019).

El Organismo de Certificación (OC) se crea con el objeto de dar cumplimiento a una de las funciones que el Real Decreto 421/2004, de 12 de marzo asigna al Centro Criptológico Nacional y su Reglamento queda recogido en la Orden de Presidencia 2740/2007, de 19 de septiembre.

El OC del CCN ha participado activamente en estos últimos 15 años en el fortalecimiento de la ciberseguridad en España mediante el establecimiento del Esquema Nacional para la Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI), el desarrollo de una metodología ligera nacional para la evaluación de productos de seguridad (LINCE) y la potenciación del ENECSTI con nuevos laboratorios de evaluación.

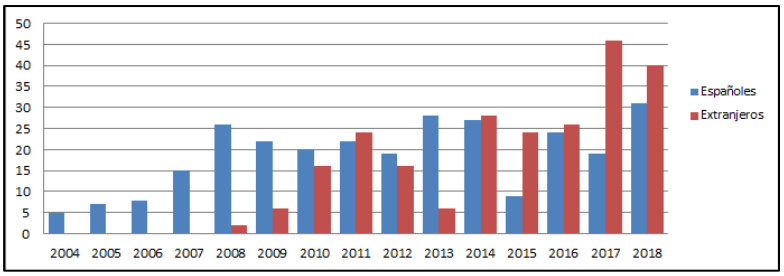
Los certificados emitidos por el OC siguen habitualmente los criterios y metodología *Common Criteria* (CC) y son reconocidos entre numerosos países a través de los acuerdos internacionales SOGIS-MRA (ámbito europeo) y CCRA (mundial).

El CCRA (*Common Criteria Recognition Arrangement*) es el acuerdo internacional de reconocimiento mutuo de certificados *Common Criteria* hasta EAL2. España firmó el acuerdo en el año 2000 y desde 2007 es miembro autorizado para la emisión de certificados reconocidos.

El SOGIS-MRA (*Senior Officers Group for Information Security – Mutual Recognition Agreement*) es el acuerdo europeo de reconocimiento mutuo de certificados hasta nivel EAL4, y hasta EAL7 para Dominios de Seguridad específicos.

La metodología LINCE es una metodología nacional de evaluación ligera, enfocada al análisis de vulnerabilidades con un esfuerzo y tiempo acotado. Está orientada a la evaluación y certificación de productos de seguridad TIC para su inclusión en el CPSTIC como producto cualificado para el ENS categoría media y básica, y también se emplea para realizar las Evaluaciones STIC complementarias de acuerdo a las guías CCN STIC-106 y CCN STIC-140.

El Organismo de Certificación desempeña su actividad desde el año 2004 admitiendo a certificación tanto productos nacionales como extranjeros, que confían en su reconocimiento internacional, llevando emitidos hasta la fecha más de 200 certificados.

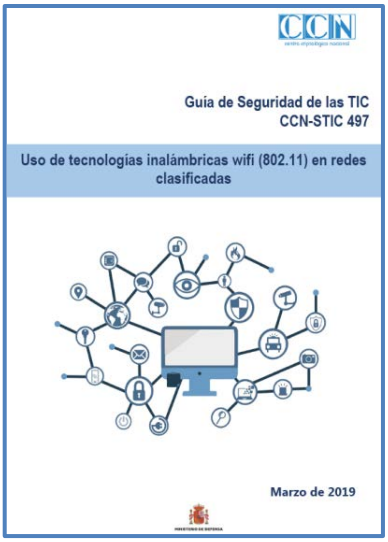


Wi-Fi Seguro

Nueva guía CCN-STIC-497 sobre empleo de Wi-Fi en redes clasificadas (03/2019).

En este documento el CCN establece un conjunto de directrices para el empleo de redes Wi-Fi 802.11 en redes clasificadas. Esta guía toma como punto de partida la arquitectura de seguridad de capas o niveles presentada en el informe de buenas prácticas CCN-CERT BP/11 sobre *Recomendaciones de seguridad en redes Wi-Fi corporativas*, y requiere que la capa destinada a proteger la confidencialidad de la información mediante un túnel cifrado (VPN/IPSec) esté implementada mediante un producto de cifra aprobado por el CCN, ya sea *hardware* o *software* dependiendo de la fortaleza de los mecanismos cripto requeridos.

La guía también plantea un análisis de la amenaza y el impacto en diversos escenarios para determinar la fortaleza de los mecanismos requeridos al producto de cifra, lo que en ocasiones podría permitir la particularización de la aprobación de productos ya incluidos en el CPSTIC para proteger información clasificada de mayor nivel en dichos escenarios.



La CCN-STIC-497 está clasificada en grado DIFUSIÓN LIMITADA debido a sus referencias explícitas a documentos con ese nivel de clasificación. Aquellos organismos y entidades que necesiten acceder a esta guía, pueden solicitarla vía correo electrónico a guias@ccn.cni.es indicando la motivación que justifica dicha petición. Una vez analizada la solicitud, si resulta procedente, el CCN remitirá el documento por los canales adecuados.

JCISAT y CCN continúan la experimentación sobre Wi-Fi seguro (02/2019).

Durante los días 26, 27 y 28 de febrero, la Sección de Arquitectura e Interoperabilidad (SECARQINT) de JCISAT/SUBCIS del Ejército de Tierra y el Centro Criptológico Nacional reanudaron las pruebas experimentales de una serie de escenarios Wi-Fi considerando tres dominios de seguridad diferenciados (RESERVADO, DIFUSIÓN LIMITADA Y SINCLAS). Dichas pruebas, continuación de las realizadas a finales de enero de este mismo año, demuestran la viabilidad de emplear de forma segura tecnologías inalámbricas que faciliten el despliegue rápido de los puestos de mando.

En esta segunda sesión experimental se emplearon los mismos productos de cifra *software* (para DL) y *hardware* (para RES) recomendados por el CCN, si bien en esta ocasión se probaron con éxito infraestructuras Wi-Fi de diversos fabricantes. Además, se solventaron las incidencias detectadas durante la primera sesión. En los próximos meses se presentan nuevos retos como la reproducción de estas pruebas en campo o el empleo de sistemas de información reales del Ejército de Tierra.

Se recuerda que esta iniciativa se enmarca dentro de los experimentos que se están desarrollando en el marco BRIEX 2035, a través del cual el Ejército de Tierra evalúa productos y tecnologías que sirvan para desarrollar su nuevo concepto de Brigada del futuro, conocido como Brigada 2035.

Productos STIC

Actualizada la taxonomía de referencia para productos de Seguridad TIC (03/2019).

El pasado mes de marzo CCN-PYTEC actualizó la taxonomía de referencia para productos de Seguridad TIC (CCN-STIC-140). Este documento pretende servir como base a la hora de establecer una taxonomía para la clasificación de productos de Seguridad en las Tecnologías de Información y la Comunicación (TIC) que forman parte activa del sistema TIC, y desarrollan su actividad en el contexto operacional de éste, implementando funcionalidades que permiten incrementar el nivel de seguridad del sistema en alguna de sus dimensiones (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad). La guía cuenta con la actualización de varios anexos, disponibles también en la parte pública del portal del Centro Criptológico Nacional, sobre los siguientes temas: Diodo de datos (D7 RFS-COM.DIO) y Dispositivos móviles (1 RFS-SER.MOV). Además, se han publicado nuevos anexos, como el de VPN-IPSec (D8.A RFS-COM.VPN.IPSec.), VPN-SSL (D8.B RFS-COM.VPN.SSL), Herramientas para la firma electrónica (E5 RFS-INF.FIR.) y Plataformas de confianza (F6 RFS-SER.PLA.).

EMSEC

Evaluación TEMPEST del Avión A330-200 MRTT (02/2019).

Durante el mes de febrero, el Grupo de Seguridad de las Emanaciones del CCN ha llevado a cabo la evaluación TEMPEST del Avión A330-200 MRTT para la empresa AIRBUS en las instalaciones de la compañía en Getafe. El uso y procesado de información clasificada, y por lo tanto la presencia de material de cifra en esta plataforma, lleva a la necesidad de confirmar que la información sensible no encuentra vías de escape a través del acoplamiento en alguno de los numerosos transmisores con los que cuenta la aeronave. El CCN dispone para este tipo de evaluaciones de un laboratorio desplegable que permite comprobar la presencia de distintas señales, tanto en las comunicaciones radio como en cables de alimentación o datos que partan de la plataforma que se esté evaluando.

Eventos

El CCN entrega el premio "Tengo un Proyecto" 2019 (03/2019).

El 8 de Marzo de 2019 tuvo lugar la entrega de los premios "Tengo un Proyecto", convocados por el Consejo Superior de Investigaciones Científicas (CSIC), con motivo del 75 Aniversario del Edificio "Leonardo Torres Quevedo". El CCN hizo entrega del premio de la especialidad de *Criptología y Seguridad de la Información* a María del Mar Giménez Aguilar por su Trabajo Fin de Master (TFM) titulado "Zephyrus: An Ethereum Steganographic Tool".

También se hizo entrega de los premios de la especialidad *de Acústica* a Joaquín García Gómez por su proyecto "Detección acústica de situaciones violentas en transporte público", y en la especialidad de *Sensores y Tecnologías Ultrasónicas* el premio recayó en Sergio Pérez Bachiller por su proyecto "Implementación Android de algoritmos de fusión sensorial para navegación de personas en espacios interiores extensos mediante el teléfono móvil". El CCN felicita a los premiados por la madurez y calidad de los trabajos presentados.

CCN-PYTEC asiste al plenario del Comité UNE-CTN 320 "Ciberseguridad y protección de datos personales" (03/2019).

La Asociación Española de Normalización (UNE) es responsable del desarrollo y difusión de las normas en España, y representante ante organismos de normalización internacionales.

El CCN-PYTEC preside dos de los seis subcomites técnicos de normalización nacionales de UNE-CTN 320 "Ciberseguridad y protección de datos personales". CCN-PYTEC aporta de esta manera sus conocimientos y experiencia en el subcomité 2 dedicado a la "Criptografía y mecanismos de seguridad", y en el subcomite 3 dedicado a la "Evaluación, pruebas y especificaciones de seguridad".

Formación online sobre el Catálogo de productos STIC (03/2019).

El próximo 5 de abril de 10:00h a 13:00h se celebrará una sesión online a través de la plataforma VANESA sobre el Catálogo de productos STIC (CPSTIC). En esta sesión se abordará el origen del CPSTIC, qué beneficios conlleva el uso del catálogo, qué productos de seguridad se pueden encontrar y cómo utilizarlo a la hora de adquirir productos de seguridad. Además, se aclarará la diferencia entre productos cualificados y certificación de conformidad con el ENS. También se presentarán las nuevas líneas de trabajo que se están desarrollando para ampliar el número de familias y productos incluidos en el catálogo. Durante la sesión sobre el Catálogo de productos STIC habrá

tiempo para resolver las dudas planteadas por los interesados que soliciten el curso y asistan a la sesión en el horario indicado.

Solicitud de curso y acceso a la plataforma

Los interesados en participar en esta actividad formativa pueden cumplimentar el formulario disponible en el siguiente enlace: formulario de inscripción. El plazo de solicitud finalizará el miércoles, 27 de marzo. No obstante, si se completasen las plazas disponibles antes de la fecha prevista se desactivará el formulario.

Contacto

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