

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

Boletín CCN-PYTEC nº29 - 04/2021

Comunicaciones Tácticas Seguras

El Ejército de Tierra comienza a emplear soluciones de cifra nacional en búsqueda del futuro Batallón RESTRICTED (03/2021).



En las Jornadas de Telecomunicaciones celebradas por la Brigada X “Guzmán el Bueno” en la Base de Cerro Murriano el pasado mes de marzo, se emplearon por primera vez los nuevos equipos de cifra nacional que servirán como base para la consecución de un Batallón acreditable a nivel NATO RESTRICTED / DIFUSIÓN LIMITADA.



En concreto se emplearon el nuevo Gestor de Comunicaciones del ET (GSCOMET v4S), que incorpora el [cifrador táctico TZ-1001](#) (familia CIFPECOM) como elemento de cifra adosado, y la nueva Unidad de Comunicaciones Seguras (UCS) que incluye en su interior el módulo de cifra TZ-501. Tanto GSCOMET v4S como la UCS son capaces de cifrar las comunicaciones de voz y datos a través de la Red Radio de Combate empleando los anteriores elementos de cifra, y transmitiendo posteriormente la información por su canal natural: la voz táctica cifrada por el canal de voz CNR de las radios y los datos cifrados por el canal de datos de las radios. GSCOMET v4S y la UCS son interoperables entre sí, y también lo serán con otras soluciones existentes para el cifrado de la información proveniente de los Sistemas de Mando y Control tales como BMS-ET.



Por otro lado, el Ejército de Tierra organizó el pasado 17 de marzo un seminario *online* para explicar este nuevo equipamiento CIS al personal de Fuerzas Armadas y del Órgano Central del Ministerio de Defensa. El Centro Criptológico Nacional participó en estas jornadas con una presentación sobre los protocolos de interoperabilidad cripto (nacional y OTAN) implementados en estos nuevos productos.

Esquema Nacional de Evaluación y Certificación STIC

Publicada la norma UNE 320001 sobre la metodología de evaluación LINCE (02/2021).



La Asociación Española de Normalización (UNE) ha publicado la [norma UNE 320001 "Metodología de evaluación LINCE para la ciberseguridad de productos TIC"](#). La UNE 320001 establece los requisitos básicos y define el marco de referencia en el ámbito de la evaluación de ciberseguridad de productos TIC. **LINCE es la primera y más reconocida certificación de ciberseguridad en España para niveles de seguridad medios y bajos**, lo que demuestra la madurez de la industria en España. Fue **desarrollada hace tres años por el CCN (Centro Criptográfico Nacional)** para poder evaluar los productos TIC de media y baja seguridad a un precio asequible por parte del desarrollador. Ahora, se convierte en un estándar UNE.

Contar con una certificación según el estándar LINCE permite, además de **mejorar la ciberseguridad del producto que se evalúa, realizarse dentro de un tiempo y esfuerzo acotados**, lo que se traduce en que sean accesibles a todo tipo de desarrolladores. Además, **posibilita el acceso al catálogo de Productos de Seguridad CPSTIC**, utilizado como referente de ciberseguridad en España para productos TIC, recomendado por el CCN.

Nuevo esquema europeo de certificación de ciberseguridad para 5G (02/2021).



La **Agencia de la Unión Europea para la Ciberseguridad (ENISA)**, tras la solicitud de la Comisión Europea, ha iniciado los [trabajos para sentar las bases de un futuro esquema de certificación de ciberseguridad específico para la tecnología 5G](#). Este nuevo esquema, que surge como parte de la iniciativa ["EU Toolbox for 5G security"](#), deberá contribuir a mejorar la ciberseguridad de las redes 5G y a mitigar ciertos riesgos asociados a la implantación de esta tecnología en la Unión Europea.

El laboratorio DEKRA acreditado para realizar evaluaciones LINCE (02/2021).



Tras superar las auditorías de la Entidad Nacional de Acreditación (ENAC) y del Organismo de Certificación del Centro Criptológico Nacional (OC-CCN), se ha publicado [en el BOE la resolución](#) que acredita a **DEKRA Testing and Certification, S.A.U.** para poder realizar **evaluaciones esenciales de seguridad (LINCE)** dentro del Esquema Nacional de Evaluación y Certificación STIC (ENECSTIC).

Eventos

Premio “Tengo un Proyecto” Criptología y Seguridad de la Información 2020 (03/2021).



La tercera edición del premio “TENGO UN PROYECTO”, del Instituto de Tecnologías Físicas y de la Información Leonardo Torres Quevedo, al mejor trabajo fin de grado o proyecto fin de máster en el área de Criptología y Seguridad de la Información, cuyo premio es patrocinado por el Centro Criptológico Nacional (CCN), ya tiene ganador.

El jurado de los Premios LTQ 2020 en Criptología y Seguridad de la Información ha decidido, por unanimidad, otorgar el premio a **Marino Tejedor Romero** por su trabajo titulado "**Sistema distribuido y remoto de votación electrónica basado en secreto compartido homomórfico de Shamir**".

A la vista de la calidad de los trabajos presentados, se han concedido **tres Menciones Especiales** a los trabajos presentados por **Ferran Alborch Escobar**, **Luis Hernández Álvarez** y **Héctor Masip Ardévol** (en orden alfabético) por sus respectivos trabajos “Lattice-based threshold cryptography”, “Towards Privacy--Preserving Sensor--Based Continuous Authentication” y “Linkable Attribute-Based Signature”.

El CCN felicita a los premiados por la madurez y calidad de los trabajos presentados.

Productos STIC

Publicada la guía CCN-STIC-1206 "Procedimiento de empleo seguro NGSiem LogICA5" (01/2021).



Se acaba de publicar la guía **CCN-STIC-1206 "Procedimiento de empleo seguro NGSiem LogICA5"** para sistemas del Esquema Nacional de Seguridad categoría ALTA.

[Puedes consultar la guía en el enlace.](#)

Publicada la guía CCN-STIC-1503 "Procedimiento de empleo seguro McAfee Data Loss Prevention" (02/2021).



Se acaba de publicar la guía **CCN-STIC-1503 "Procedimiento de empleo seguro McAfee Data Loss Prevention"** para sistemas del Esquema Nacional de Seguridad categoría ALTA.

[Puedes consultar la guía en el enlace.](#)

Publicada la guía CCN-STIC-1102 "Procedimiento de Empleo Seguro Citrix Netscaler ADC" (02/2021).



El CCN ha publicado la guía **CCN-STIC-1102 "Procedimiento de Empleo Seguro Citrix Netscaler ADC"** para sistemas a los que aplique el Esquema Nacional de Seguridad categoría ALTA.

[Puedes consultar la guía en el enlace.](#)

Publicada la guía CCN-STIC-1406 "Procedimiento de empleo seguro del Cortafuegos Fortigate" (03/2021).



El CCN ha actualizado la guía **CCN-STIC-1406 "Procedimiento de empleo seguro del Cortafuegos Fortigate"** de la empresa Fortinet para sistemas Esquema Nacional de Seguridad categoría ALTA.

[Puedes consultar la guía en el enlace.](#)

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/UCuSR7guHqx5kgoj6kafOF1Q

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