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

Boletín CCN-PYTEC nº20 - 11/2019

Novedades en el Catálogo de Productos STIC

X930 Series AlliedWare Plus, cualificado en la familia de "Switches" para ENS categoría ALTA (10/2019).

La serie de productos *X930 Series AlliedWare Plus* (*AT-x930-28GTX, AT-x930-28GPX, AT-x930-52GTX, AT-x930-28GPX, AT-x930-28GSTX*) *versión 5.4.6.1* ha sido incluida en el Catálogo de Productos de Seguridad TIC como cualificada para ENS categoría ALTA en la familia de *"Switches"*.

La familia *x930 de Allied Telesis* está formada por "*switches"* apilables que operan en capa 3 con puertos Gigabit.

ADSS Server SAM Appliance, cualificado en la familia de "Herramientas para firma electrónica" para ENS categoría ALTA (10/2019).

El *ADSS Server SAM 6.0* es un dispositivo de creación de Firma Remota (rQSCD) de la empresa Ascertia, que cuenta con un certificado *Common Criteria EAL4+,* de acuerdo al perfil de protección EN 419241-2 con *Level 2 Sole Control* y que, junto a la aplicación de móviles Go>Sign de Ascertia, proporciona a sus usuarios la firma Remota Avanzada y Cualificada.

Samsung Electronics cualifica nuevos productos en la familia de "Dispositivos móviles" para ENS categoría ALTA (10/2019).

Samsung Galaxy Note 9 y Galaxy Tab S4, ambos con la versión de Android 8, han sido incluidos en el Catálogo de Productos de Seguridad TIC como cualificado para ENS categoría ALTA en la familia de "Dispositivos móviles".

Nuevas versiones de Microsoft Windows 10 cualificadas y aprobadas (10/2019).

El producto Microsoft Windows 10 versión 1809 *Enterprise Edition* ha sido cualificado para ENS categoría ALTA, mientras que *Microsoft Windows 10 Enterprise LTSC 2019* ha sido aprobado para su uso en sistemas que manejan información clasificada.

Publicada la Guía CCN-STIC 1405 "Procedimiento de empleo seguro del IS101" (11/2019).

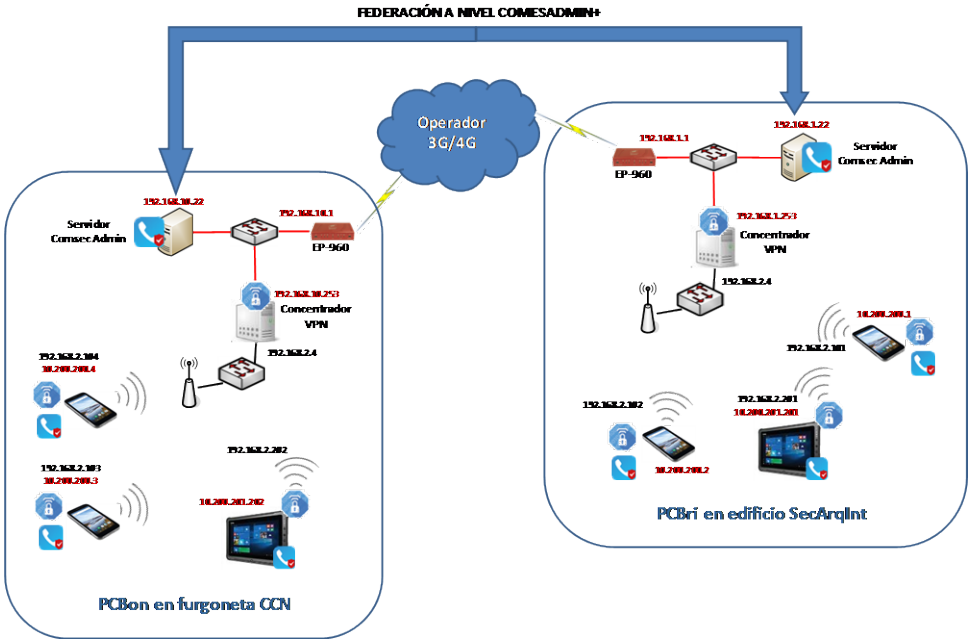
Se ha publicado el procedimiento de empleo seguro del IS101. El equipo IS101 de la empresa Istria Soluciones de Criptografía ha sido cualificado para ENS categoría Alta dentro de la familia: Redes privadas virtuales: IPSec.

El IS101 es un cifrador de altas prestaciones que, sobre una plataforma hardware segura con un FW/SW específico, implementa protocolo IPSec en modo túnel (con encapsulado ESP y protocolo IKEv2), lo que permite establecer, de forma sencilla y eficiente, redes privadas virtuales (VPN) sobre una red IP no confiable (ya sea pública o privada). Está diseñado para sistemas en entornos críticos que manejan información sensible no clasificada, proporcionando una velocidad de transferencia de 2Gbps agregados.

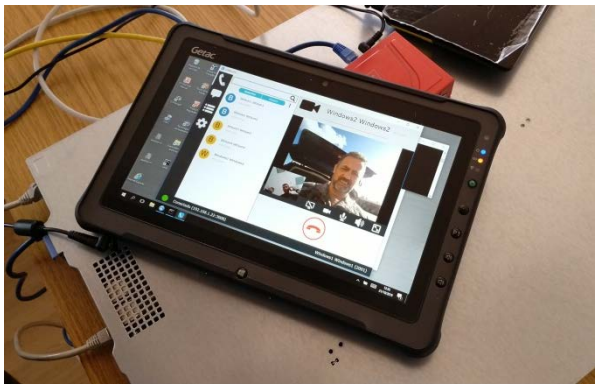
Comunicaciones Tácticas Seguras

Experimento de federación de células inalámbricas seguras para puestos de mando desplegables (11/2019).

El pasado 21 de octubre, en el marco de las pruebas conjuntas entre CCN y la JCISAT del Ejército de Tierra sobre securización de tecnologías inalámbricas (LTE, WiFi, etc.), se llevó a cabo con éxito un experimento de federación de células inalámbricas con infraestructuras de seguridad independientes. En esta ocasión se emplearon dos redes WiFi independientes securizadas con la suite de seguridad conformada por la VPN Safemove de Bittium y la aplicación ComsecAdmin+ de Indra para comunicaciones seguras de voz, datos y video. Ambas burbujas se interconectaron mediante un enlace seguro a través de cifradores de EPICOM. La federación de las dos células inalámbricas independientes permitió el establecimiento de comunicaciones "inter-burbuja" entre los clientes ComsecAdmin de las dos células, además de conectividad IP.



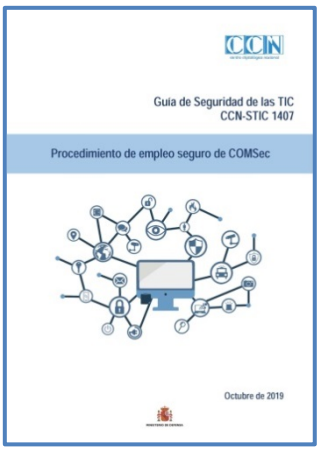
Este experimento pretendía reproducir la situación de dos puestos de mando inalámbricos seguros e independientes, uno de ellos con posibilidad de movilidad, que en determinadas situaciones necesitan establecer comunicaciones entre sí. El puesto ubicado en el edificio de la Sección de Arquitectura e Interoperabilidad de la JCISAT en el Acuartelamiento Capitán Sevillano desempeñó las funciones de un Puesto de Mando de Brigada (PCBri), mientras que el puesto ubicado en una furgoneta desempeño las funciones de Puesto de Mando de Batallón (PCBon).



También se llevó a cabo una prueba equivalente en la que la conectividad entre burbujas era prorpocinada por GESCOMET (Gestor de Comunicaciones de ET) con medios radio militares de banda ancha. En pruebas futuras se incoporarán a este escenario sistemas de información del Ejército tales como BMS-ET; además, sería deseable llevar a cabo pruebas con una Unidad Operativa y probar el enlace entre burbujas con diferentes medios de transmisión (satélite, radio-enlace, etc.).

Movilidad

Publicada la Guía CCN-STIC 1407 sobre procedimiento de empleo seguro de COMSec (11/2019).



Este documento recoge los pasos a seguir para poner en marcha el sistema COMSec, de acuerdo con las directrices establecidas por el Centro Criptológico Nacional (CCN) durante el proceso de cualificación del producto.

COMSec proporciona comunicaciones cifradas de voz, video y mensajería instantánea a usuarios móviles a través de una aplicación instalada en una plataforma Android.

Uso de servicios de movilidad seguros por parte de las Fuerzas Armadas finlandesas en zona de operaciones (11/2019).

Durante las próximas Jornadas STIC CCN-CERT (13ª edición), que tendrán lugar en Kinepolis (Madrid) los días 12 y 13 de diciembre, la empresa finlandesa Bittium presentará un caso real de uso de soluciones para comunicaciones móviles seguras en operciones internacionales por parte de sus Fuerzas Armadas (FAS). El sistema denominado FINBLUECORE, empleado por las tropas finlandesas destinadas a la gestión de crisis internacionales, emplea productos tales como los "smartphone" Bittium Tough Mobile o la VPN SafeMove. Algunos de esos productos han sido ya aprobados por el CCN para procesar información clasificada nacional tras superar las oportunas evaluaciones de seguridad, y algunos otros están inmersos en dichas evaluaciones.

La presentación tendrá lugar el día 12 de dicembre a las 10:45 dentro del módulo 3 de la Jornadas denominado "Prevención en ciberseguridad / soluciones tecnológicas".

EMSEC

El shelter SHATEM de ARPA, certificado TEMPEST para operar en zona 0 (11/2019).

El shelter SHATEM (Shelter ARPA TEMPEST Multipropósito) de la empresa ARPA Equipos Móviles de Campaña ha superado las pruebas de medidas de atenuación TEMPEST necesarias para que este shelter pueda operar en instalaciones ZONA 0. El laboratorio TEMPEST del CCN ha llevado a cabo las medidas oportunas para confirmar que los niveles de atenuación que ofrece el shelter tanto en radiadas como en conducidas, permiten trabajar en su interior con equipos comerciales con información hasta un nivel de clasificación CONFIDENCIAL o equivalente sin necesidad de evaluar ZONING dichos equipos, o bien con equipos ZONA 2 para el manejo de información clasificada RESERVADO o equivalente y superior.

El CCN participa en el Simposio de Seguridad TEMPEST y EMC del NCSC (10/2019).

National Cyber Security Centre
a part of GCHQ

El CCN ha participado a principios del mes de octubre en el Simposio 2019 de Seguridad TEMPEST y EMC organizado por el National Cyber Security Center (NCSC) de Reino Unido, en las instalaciones de los laboratorios Qinetiq en Farnboroug. Este congreso reúne a expertos TEMPEST nacionales de agencias de numerosos países, así como de OTAN, que exponen los avances e investigaciones realizadas por sus organizaciones en aspectos relacionados con la seguridad de emanaciones y TEMPEST. Como en otras ocasiones las sesiones se han centrado en aspectos de organización, política y demostraciones técnicas haciéndose un especial hincapié en la

evaluación de armarios apantallados, la seguridad de emanaciones luminosas y en la próxima versión de las normas SDIP sobre las que se está trabajando. Estas reuniones sirven además como un importante punto de encuentro de la comunidad de Seguridad de Emanaciones de cara a la formación, al establecimiento de relaciones e intercambio de conocimientos y experiencias.

OTAN y Unión Europea

El CCN asiste al CaP4 de la OTAN (10/2019).

Los días 2 y 3 de octubre el CCN participó en la reunión del *Information Assurance and Cyber Defence Capability Panel* de la OTAN, celebrada en las instalaciones del Cuartel General de la OTAN en Bruselas. El CCN representa a España en este Panel OTAN, conocido como CaP4, bajo la estructura del *C3 Board* de la OTAN. El CaP4 aconseja y apoya al *C3 Board* en todas las cuestiones relacionadas con protección de la información, ciberdefensa y las tecnologías asociadas. Este *Capability Panel* estructura sus reuniones en tres líneas de actividad diferenciadas: interoperabilidad de servicios criptográficos; evaluación de productos y certificación; y seguridad de los sistemas CIS y ciberdefensa. Cabe citar que en las últimas reuniones del CaP4 uno de los temas destacados viene siendo el plan de acción de la Alianza frente a la amenaza cuántica.

El CCN participa en CSC-IA (11/2019).

El pasado 6 de noviembre se celebró la reunión del grupo de Seguridad de la Información del Comité de Seguridad del Consejo de la Unión Europea. Este grupo es el encargado de redactar las políticas de seguridad de la información de la UE; asi como supervisar las actividades de los Estados Miembros y organismos europeos sobre esta materia. En esta reunión se ha debatido sobre las actividades de la Secretaría General del Consejo que implican el manejo de información clasificada de la UE y de la nueva normativa de la UE para la aprobación, uso y gestión de material criptográfico. El CCN ha asistido como representante nacional en dicho grupo.

Eventos

@CCNPYTEC organiza el desayuno tecnológico “Dispositivos móviles en el ENS: La base para la Transformación Digital en la Administración” (11/2019).

El pasado 14 de noviembre, en el Salón de Actos del Consejo Superior de Investigaciones Científicas (CSIC), se celebró una nueva edición de los desayunos tecnológicos que organiza el Departamento de Productos y Tecnologías del CCN.

El CCN, junto con algunos de los actores de la industria que ya han cualificado sus productos, mostraron la arquitectura propuesta para incorporar dispositivos

móviles (smartphones, tablets, equipos portátiles, etc.) en organismos del sector público y dar cumplimiento al Esquema Nacional de Seguridad. El evento contó con la participación de casi 100 organismos de la Administración.

El CCN patrocina el premio "Tengo un Proyecto" (11/2019).

El Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo", de la Agencia Estatal Consejo Superior de Investigaciones Científicas (CSIC), convoca la segunda edición del premio "Tengo un Proyecto".

El CCN patrocina el premio "Tengo un Proyecto" del Instituto de Tecnologías Físicas y de la Información "Leonardo Torres Quevedo" al mejor Trabajo Fin de Grado (TFG) o Proyecto Fin de Master (PFM), en el área de Criptología y Seguridad de la Información. Mas información en http://www.itefi.csic.es/en/premio-tengo-un-proyecto/area-criptologia-2019

CCN-PYTEC estará presente en las XIII Jornadas STIC CCN-CERT (11/2019).

El próximo 11 y 12 diciembre, CCN-PYTEC estára presente en el Módulo 3: "Prevención en ciberseguridad y Soluciones Tecnológicas" de las XIII Jornadas STIC CCN-CERT "Comunidad y Confianza, bases de nuestra ciberseguridad". Este módulo será inaugurado con la ponencia "Cybersecurity Act" que será impartida por el Departamento de Productos y Tecnologías del CCN.

El evento evento tendrá lugar los días 11 y 12 de diciembre en Kinépolis de Madrid (Ciudad de la Imagen). El evento es gratuito, aunque el acceso a las Jornadas está sujeto a la validación de la solicitud por parte de la organización. El aforo para la edición de este año ya está completo.

Además del módulo de prevención en ciberseguridad y soluciones tecnológicas, en esta edición, se abordarán las siguientes temáticas:

- Módulo 1: Amenazas, ataques y retos tecnológicos
- Módulo 2: ENS y Cumplimiento Normativo
- Módulo 3: Prevención en ciberseguridad y Soluciones Tecnológicas
- Módulo 4: Atenea, sala de retos (en colaboración con RootedCon)
- Módulo 5: Operaciones Militares en el Ciberespacio (en colaboración con el Mando Conjunto de Ciberdefensa)
- Módulo 6: Redes Operacionales y Control Industrial (en colaboración con CCI)
- Módulo 7: Desinformación/Ciberdelincuencia (en colaboración con C1b3rwall).

Contacto

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