Praeventio sit vincere

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.

Cifra IP

El cifrador EP430GN en sus versiones 1.12 y 2.04 aprobadas para NATO SECRET (10/2021).

El cifrador IP de alta velocidad **EP430GN de la empresa EPICOM**, en sus **versiones 1.12 y 2.04**, fue **aprobado** el pasado mes de octubre por el "NATO Military Committee" (NAMILCOM) para protección de información clasificada de la alianza **hasta grado NATO SECRET**.

Epicom

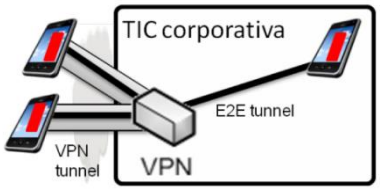
La versión 1.12 mejora la funcionalidad del equipo, solucionando algunos "bugs" de funcionamiento detectados y mejorando la estabilidad del criptosistema. La versión 2.04, además de las mejoras de la versión 1.12, incorpora un nuevo hardware al equipo, el cual sustituye aquellas partes del cifrador que habían quedado obsoletas por componentes modernos que permitirán alargar la vida útil de este equipo.

Comunicaciones Móviles Seguras

Primeras pruebas 5G "Stand Alone" con terminales seguros Färist Mobile (12/2021)

Este mes de diciembre se han realizado en la sede de Telefónica las **primeras pruebas con tecnología 5G SA ("Stand Alone")**, que incluye tanto el acceso radio como el equipamiento "core" de 5G, **empleando terminales móviles seguros Färist Mobile**.

Con esta nueva tecnología 5G SA se reduce la latencia, incrementando la capacidad de transmisión de datos. Además, gracias al sistema de comunicaciones móviles seguras Färist Mobile, se protege tanto la comunicación como el dispositivo móvil para almacenar información clasificada hasta el grado de Difusión Limitada.



El Centro Criptológico Nacional ha participado en dichas pruebas, **en las bandas de frecuencia de 700MHz y 3,5 GHz**, realizando test de llamadas, PTT ("Push To Talk") y videollamadas de forma satisfactoria. Estas pruebas se realizaron con las **aplicaciones ComsecAdmin+ y PTTSec de INDRA SCS**.

Comunicaciones Tácticas Seguras

Aprobados grado DIFUSIÓN LIMITADA los productos TZ-1001R y UCS con módulo de seguridad TZ-501 (10/2021).

El pasado mes de octubre se incluyeron en el Catálogo de Productos STIC del CCN los productos TZ-1001R versión 4.26, de la empresa Tecnobit, y la Unidad de Comunicaciones Seguras (UCS) versión 2.4 con módulo de seguridad TZ-501 versión 4.26, de las empresas RF Española y Tecnobit. Ambos productos están **aprobados para la protección de información clasificada de grado DIFUSIÓN LIMITADA hasta finales del año 2023**, momento en el cual se revisará la vigencia de dicha aprobación a fin de valorar la fortaleza de los productos frente a las nuevas amenazas que hayan podido surgir.

El TZ-1001R se puede emplear como elemento de cifra del Gestor de Comunicaciones del Ejército de Tierra (GESCOMET) versión 4S para cifrar de forma simultánea varios flujos de voz táctica ("push to talk") según varios estándares OTAN, pudiendo elegirse en cada caso el más adecuando según el tipo de radio por el que se va a realizar la transmisión. Simultáneamente también puede cifrar datos IP unicast y multicast mediante un protocolo específico de cifra IP autenticada, orientado a facilitar la integración con los sistemas CIS de dotación. Por su parte, la UCS proporciona una solución con un factor de forma menor (permite la conexión a dos radios) equivalente e interoperable con GESCOMET v4s.

Durante los primeros meses de 2022 está prevista la inclusión de estos productos en el "NATO Information Assurante Catalogue" (NIAPC) como productos aprobados para proteger información clasificada de la alianza de grado NATO RESTRICTED.

Asimismo, durante el año 2022, se evaluarán los aspectos ciber del GESCOMET v4s a fin de poder otorgar una aprobación de grado DIFUSIÓN LIMITADA a toda la solución, y así facilitar la acreditación de los sistemas donde GESCOMET se emplee.

El CCN da apoyo al Mando Conjunto de Operaciones Especiales en la ejecución de SOFEX-21 (11/2021)

El pasado mes de noviembre el Mando Conjunto de Operaciones Especiales (MCOE) llevó a cabo el ejercicio SOFEX-21 para adiestrarse como Mando Componente Nacional. El despliegue se llevó a cabo entre la Base de Retamares (Madrid) y la zona de San Roque-Cádiz y participaron unidades del Mando de Operaciones Especiales (MOE) del Ejército de Tierra, de la Fuerza de Guerra Naval Especial (FGNE) de la Armada, del Escuadrón de Zapadores Paracaidistas del Ejército del Aire (EZAPAC), así como helicópteros de las FAMET y de la Flotilla de Aeronaves de la Armada, embarcaciones de la Armada, medios RPAS, incluyendo unidades de apoyo de combate y de apoyo logístico, provenientes de los Ejércitos y la Armada.

El Centro Criptológico Nacional participó en el ejercicio facilitando y configurando equipos de cifra de la empresa EPICOM y diodos de la empresa AUTEK. Los cifradores **EP960 de EPICOM** se emplearon para proteger la transmisión del ISR del dron Scan-Eagle entre la "Ground Control Station" (GCS) y la Base de Operaciones Avanzada (BOA), así como con el Centro de Mando del MCOE en Retamares. Por otra parte, los **diodos PSTDiode de AUTEK** se emplearon para la integración segura de la información GEOINT en el Sistema de Mando Clasificado.

Nube segura

Arquitecturas marco para el manejo de información clasificada en la nube (12/2021)

El Centro Criptológico Nacional está trabajando en la definición de dos arquitecturas marco para el manejo de información clasificada en la nube.

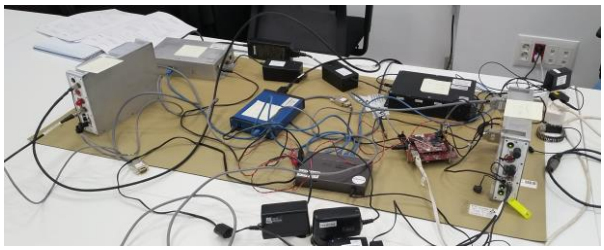
Por un lado, se definirá una arquitectura marco para el manejo de información clasificada con nivel alto nivel de clasificación basándose en el concepto de nube segura. Se define el concepto de nube segura como una nube con las siguientes características:

- Nube privada: nube de uso exclusivo por parte del "Cloud Service Customer" (CSC) y sus organismos afines y/o dependientes.
- Nube aislada: nube desconectada de los "Cloud Service Providers" (CSP) de nube pública y otras redes públicas.
- Nube controlada: las comunicaciones y los servidores tipo nube deben estar alojados en instalaciones bajo la supervisión y el control del CSC.
- Nube gestionada: el personal que gestione los servidores y servicios de la nube debe ser nacional y disponer de las adecuadas habilitaciones de seguridad, aunque se trate de personal del CSP.

Por otro lado, se definirá una arquitectura marco para manejar información con bajo nivel de clasificación que se podrá desplegar en sistemas de nube pública. Para esta arquitectura marco, se está desarrollando un piloto en AWS para estudiar la viabilidad del despliegue de herramientas y soluciones de seguridad aprobadas para el manejo de información clasificada en sistemas Cloud y adaptarlas en su caso para ponerlas a disposición de la administración.

Sistemas GNSS Seguros

Nuevo módulo de seguridad de Canal Secundario para el receptor nacional PRESENCE2 (12/2021).



Durante este año 2021 **la empresa Tecnobit ha desarrollado un módulo de seguridad para integrar el receptor PRESENCE2**, primer receptor nacional operacional de Servicio Público Regulado (PRS) Galileo, **bajo la estructura de gestión del Canal Secundario nacional**.

Dicho **Canal Secundario** está siendo **desplegado por el INTA en sus funciones como CPA española (Autoridad Competente en PRS), y ofrece la posibilidad de complementar y mejorar la señal primaria procedente de los satélites** (p.ej. optimización de los tiempos de envío de mensajes a los receptores), gestionar los receptores PRS nacionales (enviándoles órdenes específicas, "re-key" por el aire, envío de mensajes de anulación del servicio a receptores perdidos, etc.) sin necesidad de que se realice a través del GSMC y otros centros de control de Galileo, lo cual incrementa la soberanía nacional sobre el sistema. **Además, este Canal Secundario permite a los receptores nacionales contar con un canal de retorno de datos (p.ej. posición, velocidad y tiempo - PVT).**

El módulo de seguridad de Canal Secundario (C2-SM) desarrollado por Tecnobit proporciona las anteriores capacidades al receptor PRESENCE2, habiéndose llevado a cabo las primeras pruebas con señal real en las instalaciones de la CPA durante este mes de diciembre. Con este nuevo C2-SM se facilitará la gestión del receptor PRESENCE2 en los diferentes sistemas de navegación donde está previsto su uso (sistema SENDA en la F110, sistemas ISNAV en el VCR 8x8, etc.).

Taxonomía de referencia para productos y Servicios STIC

Actualizada la Guía CCN-STIC 140 Taxonomía de referencia para productos STIC (10/2021).

Se ha actualizado la Guía CCN-STIC 140 Taxonomía de referencia para productos STIC que categoriza aquellos productos TIC que forman parte de la arquitectura de seguridad de los sistemas TIC y define unos Requisitos Fundamentales de Seguridad.

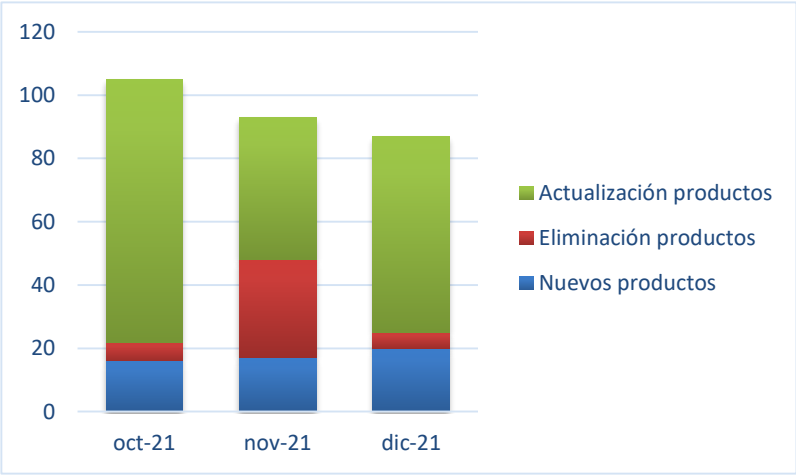
Para cada familia de productos de la taxonomía se ha definido un documento de Requisitos Fundamentales de Seguridad (RFS), que deberían tomarse como referencia para el desarrollo, evaluación y uso seguro de los productos dentro de cada familia. Estos RFS se incluyen en los anexos de esta guía (Puedes consultar los RFS en el siguiente enlace)
En la actualización realizada en el mes de octubre de 2021 se encuentran disponibles 5 nuevos RFS:

- A4 Servidores de Autenticación (cat. ALTA)
- A4M Servidores de Autenticación (cat. MEDIA)
- B3 Herramientas de gestión de red (cat. ALTA)
- B3M Herramientas de gestión de red (cat. MEDIA)
- E6 *Hardware Security Module* (HSM) (cat. ALTA)

Novedades CPSTIC

Novedades en las publicaciones del último trimestre de 2021 del Catálogo de Productos y Servicios STIC (CPSTIC)

Con el objetivo de proporcionar a los organismos públicos productos y servicios STIC actualizados, el CPSTIC se actualiza de forma mensual con nuevos productos cualificados o aprobados. Durante este periodo se han incluido **53 nuevos productos en el CPSTIC**.
De forma global, en el último trimestre de 2021, se han producido un total de 285 movimientos en el CPSTIC entre altas, bajas y actualizaciones.



Procedimientos de Empleo Seguro publicados

Publicada la guía CCN-STIC-1106 "Procedimiento de empleo seguro de Forescout CounterACT v8.1" (09/2021).

Se ha publicado la guía CCN-STIC-1106 "1106 Procedimiento de empleo seguro Forescout CounterACT v8.1", como Herramienta de Control de Acceso a Red para sistemas Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1210 "Procedimiento de empleo seguro de RSA NetWitness Platform 11" (10/2021).

Se ha publicado la guía CCN-STIC-1210 "Procedimiento de empleo seguro de RSA NetWitness Platform 11", como SIEM para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1420 "Procedimiento de empleo seguro de Sonicwall SonicOS" (10/2021).

Se ha publicado la guía CCN-STIC-1420 "Procedimiento de empleo seguro de de Sonicwall SonicOS como Cortafuegos, IPS y VPN-IPSEC para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1610 "Procedimiento de empleo seguro de KATUA SDI Platform" (10/2021).

Se ha publicado la guía CCN-STIC-1610 "Procedimiento de empleo seguro de KATUA SDI Platform" como herramienta de hiperconvergencia para sistemas del Esquema Nacional de Seguridad (ENS) categoría MEDIA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1421 "Procedimiento de empleo seguro de WatchGuard Fireware OS v12.6.2" (11/2021).

Se ha publicado la guía CCN-STIC-1421 "Procedimiento de empleo seguro de WatchGuard Fireware OS v12.6.2 como cortafuegos y redes privadas virtuales: IPSec para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1422 "Procedimiento de empleo seguro de Allied Ware Plus (AW+) versión 5.5.0-0.6" (11/2021).

Se ha publicado la guía CCN-STIC-1422 "Procedimiento de empleo seguro de Allied Ware Plus (AW+) versión 5.5.0-0.6 como Switches para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1108 "Procedimiento de empleo seguro de CyberArk Privileged Account Security Solution" (12/2021).

Se ha publicado la guía CCN-STIC-1108 "Procedimiento de empleo seguro de CyberArk Privileged Account Security Solution como herramienta de Gestión de Acceso Privilegiado (PAM) para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1507 "Procedimiento de empleo seguro de Forcepoint On-Premise Security 8.5" (12/2021).

Se ha publicado la guía CCN-STIC-1507 "Procedimiento de empleo seguro de Forcepoint On-Premise Security 8.5 como herramienta de proxy y sistemas para la prevención de fugas de datos para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1103 "Procedimiento de empleo seguro de Aruba ClearPass 6.9" (12/2021).

Se ha publicado la guía CCN-STIC-1103 "Procedimiento de empleo seguro de Aruba ClearPass 6.9 como Dispositivos de Control de Acceso a Red y Servidores de Autenticación para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA.

Puedes consultar la guía en el enlace.

Publicada la guía CCN-STIC-1506 "Procedimiento de empleo seguro de EP880" (12/2021).

Se ha publicado la guía CCN-STIC-1506 "Procedimiento de empleo seguro de EP880 como herramienta de cifrado offline para sistemas del Esquema Nacional de Seguridad (ENS) categoría ALTA y para sistemas que manejan información clasificada hasta DIFUSIÓN LIMITADA.

Puedes consultar la guía en el enlace.

CCN-PYTEC

centro criptológico nacional

ccn-pytec@cni.es

@CCNPYTEC

https://www.linkedin.com/company/CCN-PYTEC

youtube.com/channel/UCuSR7guHgx5kgoj6kafOF1Q