

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

Boletín CCN-PYTEC nº25 - 08/2020

Esquema Nacional de Evaluación y Certificación STIC

ENISA ha publicado el Esquema Europeo para la certificación de la ciberseguridad basada en Common Criteria (EUCC) (07/2020).

ENISA (“European Union Agency for Cybersecurity”) ha lanzado una [consulta pública sobre el primer candidato para el Esquema Europeo de certificación de ciberseguridad](#). Se trata del Esquema Europeo para la certificación de la ciberseguridad basado en Common Criteria (EUCC).



APPLUS, laboratorio Common Criteria EAL6+ (07/2020).



Tras superar las auditorías de ENAC y del Organismo de Certificación del CCN, el laboratorio APPLUS está acreditado para realizar evaluaciones funcionales de seguridad Common Criteria hasta nivel EAL6+. [La resolución de la Secretaria de Estado Directora del CCN fue publicada en el BOE](#) el pasado día 8 de julio de 2020. Este laboratorio, perteneciente al Esquema

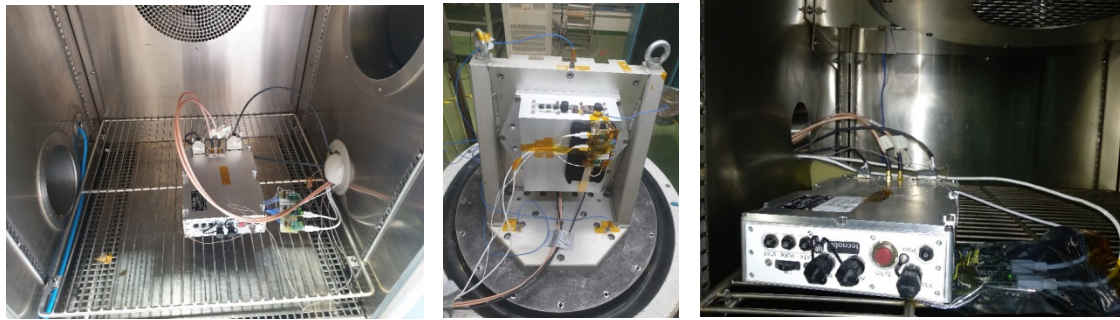
Nacional de Evaluación y Certificación STIC (ENECSTIC), también está acreditado para la realización de evaluaciones LINCE.

Sistemas Seguros de Navegación por Satélite

Primera evaluación cripto de un módulo de seguridad PRS nacional (06/2020).



El pasado mes de junio, TECNOBIT remitió la solicitud formal de certificación y aprobación del módulo de seguridad de PRS del receptor PRESENCE2. Se trata de un nuevo equipo que incluye las medidas de seguridad tanto lógicas como físicas para proteger los activos del servicio PRS en operaciones, cumpliendo los estándares de la UE para nivel SECRET. Una vez se completen las actividades asociadas al proceso de aprobación nacional de este producto, será necesario superar una segunda evaluación de la autoridad de certificación criptológica de una nación AQUA (“Appropriately Qualified Authority”) para la consecución de la aprobación UE SECRET.



Previo a los trabajos de certificación, TECNOBIT ha estado cualificando el módulo de seguridad desde marzo a junio, pasando satisfactoriamente pruebas ambientales de temperatura de operación, temperatura de almacenamiento, vibraciones, niebla salina, lluvia, polvo y EMI/EMC. Con ello, el módulo de seguridad que preparado para futuras integraciones en plataformas tanto terrestres como navales.

Comunicaciones móviles seguras

COMSec Admin+ de INDRA incluido en el NIAPC (08/2020).

La herramienta COMSec Admin+ de INDRA ha sido [incluida en el "NATO Information Assurance Product Catalogue" \(NIAPC\)](#) recientemente.

Este producto, que también está incluido dentro del Catálogo de Productos STIC del CCN (CPSTIC), es una solución global de comunicaciones seguras que proporciona servicios cifrados de voz, mensajería instantánea y videoconferencia sobre teléfonos móviles empleando cualquier red celular, inalámbrica o satelital.



Novedades en el Catálogo de Productos STIC

EP852 de EPICOM aprobado en la familia de "Cifrado offline" hasta CONFIDENCIAL (07/2020).

El EP852 es un cifrador de ficheros fuera de línea que permite el cifrado y descifrado de ficheros y el transporte de información cifrada en el dispositivo. Mejora las prestaciones en cuanto a almacenamiento y velocidad de las versiones anteriores de los Token USB así como la puesta en marcha del dispositivo, carga y distribución de claves.



Cifrado offline

Cisco Identity Services Engine (ISE) cualificado en la familia de “Control de Acceso a Red (NAC)” para ENS categoría ALTA (07/2020)

Cisco Identity Services Engine Appliance 3515, 3595, 3615, 3655, 3695

Cisco Identity Services Engine Virtual Machine (ISE-VM) en ESXi 6.7 ejecutado sobre UCSC-C220-M5SX

Cisco Identity Services Engine ejecutado sobre Cisco Application Deployment Engine (ADE) Release 3.0 operating system (ADE-OS)

Cisco ISE es una plataforma de control de acceso que combina la autenticación, autorización y trazabilidad (AAA), así como la gestión de usuarios, en un appliance. ISE permite control de acceso seguro en las conexiones cableadas, inalámbricas y VPN. Permite realizar búsquedas en la red para dar visibilidad sobre quién o qué accede a los distintos recursos.

Control de Acceso a Red (NAC)



Cisco Network Convergence System 5500 Series cualificado en la familia de “Enrutadores” para ENS categoría ALTA (07/2020)

NCS5504

NCS5508

NCS5516

NCS-55A1-36H-S

NCS-55A1-36H-SE-S

Cisco Network Convergence System 5500 Series es un producto de routing, usado principalmente para agregar tráfico en redes WAN (Wide Area Network). Proporciona funcionalidades de redundancia, enrutamiento de segmentos de red y gestión de redes programables.

Enrutadores

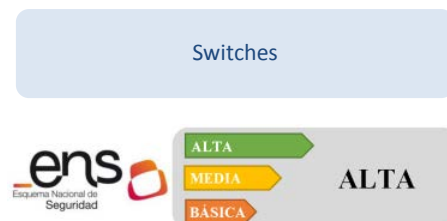


El producto ejecuta el sistema operativo IOS-XR, diseñado para procesar el tráfico de red sin sufrir retrasos de buffering.

Juniper Networks cualifica sus productos en la familia de "Switches" para ENS categoría ALTA (07/2020).



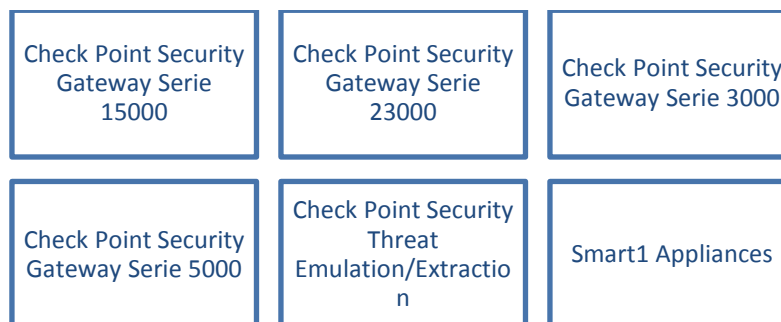
Los switches EX son dispositivos de red que soportan la definición, y cumplimiento, de las políticas de flujo de información entre los nodos de la red. Junto a funciones de seguridad del tránsito de información, el producto registra todas las actividades relevantes, y cuenta con herramientas de seguridad para la gestión de las funcionalidades de seguridad.



Como switch de nivel 2 en la capa OSI, realiza un análisis de los paquetes entrantes, reenviando dichos paquetes en función de la información que contienen, haciéndolos llegar así a su destinatario.

Como switch de nivel 3 en la capa OSI, admite el enrutamiento del tráfico basado en tablas identificando las rutas disponibles, las condiciones, la distancia y los costes para así determinar la ruta más adecuada para cada paquete.

Checkpoint cualifica sus productos en la familia de "Cortafuegos" y "Redes privadas virtuales: IPSec" para ENS categoría ALTA (07/2020).

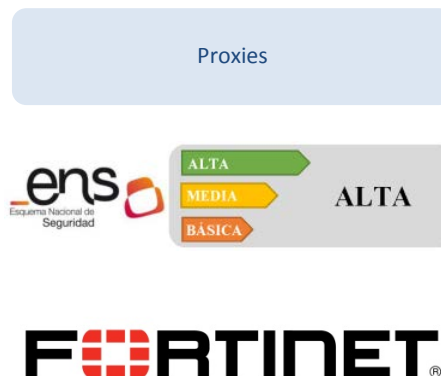


La solución Check Point Security Gateway incorpora un firewall de próxima generación (Next Generation Firewalls, NGFW) de Check Point que se centra en mejorar las tecnologías de prevención de amenazas, incluidas las funciones de emulación a nivel de CPU y antirransomware, por lo que ofrecen la seguridad más innovadora y eficaz en todos los segmentos de red y así mantienen a los clientes protegidos frente a cualquier amenaza, en cualquier momento y en cualquier lugar.



Fortinet FortiProxy cualificado en la familia de "Proxies" para ENS categoría ALTA (07/2020).

A medida que las ciberamenazas se van haciendo más sofisticadas, las compañías necesitan cada vez más una aproximación integral para proteger a los usuarios del tráfico web malicioso, los websites peligrosos y aquel contenido que pueda suponer una amenaza para ellos. El Secure Web Gateway (SWG) de Fortinet, FortiProxy, aborda esta situación con un único producto que incluye URL filtering, protección contra amenazas avanzadas y malware, filtrado DNS, DLP, IPS... La protección de los usuarios contra amenazas procedentes de internet facilita el cumplimiento de las políticas corporativas.



Aruba Virtual Intranet Access (VIA) Client cualificado en la familia de "Redes privadas virtuales: IPSec" para ENS categoría ALTA (07/2020).

Aruba Virtual Intranet Access (VIA) es un servicio VPN seguro para usuarios que necesitan conectividad corporativa remota desde el hogar, ubicaciones temporales o mientras están en movimiento. Se encuentra disponible como una descarga de software para Google Android, Apple iOS, MacOS, Linux y Windows.

La función cualificada del VIA es la de cliente VPN IPSEC que evalúa y selecciona automáticamente la mejor conexión segura para efectuar la conexión VPN con la organización. A diferencia de las VPN tradicionales que requieren hardware dedicado (terminadores de túneles), Aruba integra servicios VPN directamente en la infraestructura segura existente de Aruba (Mobility Controllers) para simplificar la arquitectura y la administración.



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/UCuSR7guHgx5kgoj6kafOF1Q

**#SALIMOS
MÁS
FUERTES**