



***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.***

## Productos de Cifra

### Aprobado el software de cifrado off-line EP880 para grado DIFUSIÓN LIMITADA (08/2021).

El [software de cifrado off-line EP880](#), desarrollado por la empresa EPICOM, ha sido **aprobado** por el Centro Criptológico Nacional (CCN) **para la protección de Información Clasificada de grado Difusión Limitada**. Además, el producto se ha **calificado para sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS) hasta categoría ALTA**.

El EP880 se ejecuta en un ordenador con sistema Windows y permite proteger archivos asegurando su confidencialidad, integridad y autenticidad. Su funcionamiento es similar a PGP, si bien emplea primitivas criptográficas más robustas cuya implementación ha sido verificada por el CCN en la pertinente evaluación criptológica.

Cuando se requiera el manejo y la protección de información clasificada DIFUSIÓN LIMITADA, el EP880 deberá emplearse en una estación de trabajo acreditada a ese nivel, ya se trate de un equipo aislado o una estación dentro de una red acreditada. No obstante, para sacarle mayor partido a la aplicación, es posible emplearlo en ordenadores no acreditados para proteger información sensible que no está clasificada formalmente, dando a esta información una protección adicional.

Aunque no tiene coste para los usuarios, el uso de este software se limita a organismos de la Administración o empresas contratistas de estos que colaboren en proyectos que requieran el manejo de Información Clasificada o información sensible del ámbito del ENS.



### Próxima aprobación OTAN de las versiones 1.12 y 2.04 del cifrador EP430GN (09/2021).

El cifrador IP de alta velocidad EP430GN de la empresa EPICOM, en sus versiones 1.12 y 2.04, recibirá en próximas fechas la aprobación de OTAN para la protección de información clasificada hasta grado NATO SECRET. 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.



Epicom

## Esquema Nacional de Evaluación y Certificación STIC

El laboratorio JTSEC acreditado para realizar evaluaciones Common Criteria (08/2021).



Tras superar las auditorías de la Entidad Nacional de Acreditación (ENAC) y del Organismo de Certificación del Centro Criptológico Nacional (OC-CCN), el pasado 19 de agosto de 2021 [se publicó en el Boletín Oficial del Estado \(BOE\)](#) la resolución que acredita al laboratorio jtsec Beyond IT Security a poder realizar evaluaciones Common Criteria dentro del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI).

## Comunicaciones Tácticas Seguras

Se aprueba para grado DIFUSIÓN LIMITADA la radio para el combatiente Bittium Tough SDR Handheld (08/2021).



**Bittium**



[La radio táctica para el combatiente Tough SDR Handheld](#) de la empresa finlandesa **Bittium Wireless Ltd.**, ha sido **aprobada** por el Centro Criptológico Nacional (CCN) para la **protección de Información Clasificada de grado Difusión Limitada**.

Se trata de una radio militar V-UHF de mano basada en tecnología SDR conforme a la arquitectura ESSOR SCA. Esta radio, en función de la forma de onda empleada, proporciona diferentes servicios de comunicaciones de voz y datos con unas prestaciones determinadas en términos de ancho de banda, alcance, número de nodos soportados en la red radio, etc.

La Tough SDR Handheld cubre la banda de frecuencias desde 30 MHz hasta 2,5 GHz y puede ejecutar formas de onda tanto de banda estrecha como de banda ancha, las cuales incluyen diferentes mecanismos de protección COMSEC, TRANSEC y NETSEC. **La evaluación criptológica** llevada a cabo por el CCN, entre otros aspectos, **ha verificado los mecanismos de la forma de onda de coalición High Data Rate Waveform** desarrollada en el [programa ESSOR \(“European Secure Software defined Radio”\)](#) en el que España participa. La aprobación para la protección de información clasificada nacional es aplicable cuando el producto se emplee con esta forma de onda.

## EMSEC

Actualizada la CCN-STIC-104 “Catálogo de Productos con clasificación ZONING” (08/2021).



Se ha actualizado la guía CCN-STIC-104 “Catálogo de Productos con clasificación ZONING” a agosto de 2021. Se han incluido nuevos equipos y sistemas evaluados en los últimos meses. Este catálogo facilita la selección de equipamiento informático que pueda cumplir con una determinada clasificación ZONING. Es de aplicación para equipos que deban manejar información clasificada NATO CONFIDENTIAL / EU CONFIDENTIAL / CONFIDENTIAL, o superior, y vayan a ser instalados en locales con clasificación ZONING de ZONA 1 o superior.

## Procedimientos de Empleo Seguro publicados

Publicada la guía CCN-STIC-1105 “Procedimiento de empleo seguro de EMMA” (07/2021).



Se ha publicado la guía CCN-STIC-1105 “Procedimiento de empleo seguro de EMMA”, herramienta de control de acceso a red (NAC), para sistemas del Esquema Nacional de Seguridad categoría ALTA.

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

Publicada la guía CCN-STIC-1505 “Procedimiento de empleo seguro de Cryhod” (07/2021).



Se ha publicado la guía CCN-STIC-1505 “Procedimiento de empleo seguro de Cryhod”, herramienta de almacenamiento cifrado de datos, para sistemas del Esquema Nacional de Seguridad categoría ALTA.

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

Publicada la guía CCN-STIC-1107 “Procedimiento de empleo seguro de *One Identity Manager*” (08/2021).



Se ha publicado la guía CCN-STIC-1107 “Procedimiento de empleo seguro de One Identity Manager”, herramienta de Gestión de Identidades (IM), para sistemas del Esquema Nacional de Seguridad categoría ALTA.

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

Publicada la guía CCN-STIC-1208 “Procedimiento de empleo seguro *McAfee Endpoint Security*” (08/2021).



Se ha publicado la guía CCN-STIC-1208 “Procedimiento de empleo seguro *McAfee Endpoint Security*” para sistemas del Esquema Nacional de Seguridad categoría ALTA.

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

Publicada la guía CCN-STIC-1303 “Procedimiento de empleo seguro *McAfee ATD*” (08/2021).



Se ha publicado la guía CCN-STIC-1303 “Procedimiento de empleo seguro *McAfee ATD*” para sistemas del Esquema Nacional de Seguridad categoría ALTA.

McAfee ATD ha sido cualificado en la familia de *Herramientas de Sandbox*.

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

## Cualificación de productos STIC destacados

### *SIAVAL Safecert Server Signing Sistema v2.4.02 (08/2021).*



**Familia:** Herramientas para Firma Electrónica

Solución de firma centralizada de la familia SIAVAL orientada a facilitar la gestión y el uso de las claves privadas y públicas de los usuarios finales, también identificados como titulares o firmantes. Está diseñado para funcionar como un dispositivo remoto de creación de firma rQSCD, según los requisitos especificados en el Reglamento (UE) nº 910/2014 del Parlamento Europeo (eIDAS: Anexo II), haciendo posible la generación de firmas electrónicas avanzadas (AdES) y de firmas electrónicas cualificadas o reconocidas (QES) en un servidor remoto.

### *SonicWall TZ Serie (300P, 350, 350W, 600P) 6.5.4.4-44n-federal-12n (08/2021).*



**Familias:** Cortafuegos, VPN IPSEC e IDS/IPS

La serie TZ de SonicWall ofrece seguridad y rendimiento de entorno Enterprise orientado a pequeñas compañías. Enfocado a entornos departamentales o PYMES de entre 5 y 100 usuarios (aprox), incorpora funciones de prevención de intrusiones, antimalware, filtrado de contenidos/URL y control de aplicaciones a través de redes y entornos inalámbricos. Proporciona inspección profunda de paquetes (DPI), SD-WAN y despliegue zero-touch. Opciones de puertos PoE y wifi 802.11ac.

### *SonicWall SOHO Serie (250, 250W) 6.5.4.4-44n-federal-12n (08/2021).*



**Familias:** Cortafuegos, VPN IPSEC e IDS/IPS

Los cortafuegos de la serie TZ SOHO de Sonicwall son una solución adecuada para oficinas pequeñas y domésticas, así como para entornos distribuidos en ubicaciones remotas. Despliegan funcionalidades para construir Secure SD-WAN y conectividad WIFI (opcional). El SOHO 250 proporciona un 50% más de rendimiento sobre su antecesor SOHO, así como acceso a los sandboxes avanzados Capture ATP, con lo que se mejora la seguridad en prevención y detección de malware desconocido en un entorno remoto.

### *Aruba Mobility Controller (9004, 7005, 7008, 7010, 7024, 7030, 7205, 7210, 7220, 7240, 7240XM, 7280) y puntos de acceso. ArubaOS 8.6 (07/2021).*



**Familias:** Cortafuegos, Dispositivos de Red Inalámbricos, VPN IPSEC

Aruba Mobility Controller Series funcionan como gateway entre redes cableadas e inalámbricas y proveen funciones de comando y control sobre los puntos de acceso de Aruba (APs) dentro de una red inalámbrica Aruba. Los Mobility Controllers (MC) y Virtual Mobility Controllers (VMC) de Aruba, son switches inalámbricos (Appliance físicos o virtuales) que proporcionan una amplia gama de servicios y características de seguridad que incluyen la movilidad de red inalámbrica y cableada, seguridad, administración centralizada, auditoría, autenticación, acceso remoto seguro, auto-chequeos de integridad y operación, filtrado de tráfico y funcionalidad de Gateway VPN.

*McAfee Web Gateway 10.0.4-35792 (07/2021).*



**Familia:** Proxies

McAfee Web Gateway proporciona una seguridad web de alto rendimiento a través de un appliance local que puede desplegarse como hardware dedicado o máquina virtual. Implementa directivas de uso de internet, analiza la naturaleza y la intención del contenido y el código activo que entra en las redes. Detecta de forma proactiva el malware zero-day gracias a la cobertura completa del tráfico web, incluido el SSL.

*EP880 V2.08.36 y V2.09.35 (07/2021).*



**Familia:** Cifrado offline

El EP880 es una aplicación software que se ejecuta sobre ordenador con sistema operativo Windows y que permite realizar, en origen, el cifrado y firma de ficheros de datos "off-line" almacenados en el disco duro del ordenador o dispositivos de almacenamiento externos conectados al ordenador, para su posterior almacenamiento y/o envío de forma segura desde el correo electrónico u otro medio y, en destino, el descifrado y verificación de la integridad de los datos.

# CCN-PYTEC

centro criptológico nacional



[ccn-pytec@cni.es](mailto:ccn-pytec@cni.es)



[@CCNPYTEC](https://twitter.com/CCNPYTEC)



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



[youtube.com/channel/UCuSR7guHgx5kgoj6kaf0F1Q](https://youtube.com/channel/UCuSR7guHgx5kgoj6kaf0F1Q)