



centro criptológico nacional

Productos de Seguridad. Nuevos desarrollos.

*I Encuentro del ENS.
Tendencias y Políticas de Seguridad*

JUNIO – 2019

CCN-pytec

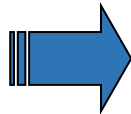


Índice

1. Breve introducción
2. Los inicios
3. La evolución
4. La actualidad. Nuevos desarrollos y CPSTIC
5. Agradecimientos
6. Consideraciones finales

1. Breve introducción

Marco legal del CCN



[Real Decreto 421/2004, de 12 de marzo](#), que regula el Centro Criptológico Nacional, define el ámbito de actuación y las funciones del CCN, y establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica

Artículo 1. *Del Director del Centro Criptológico Nacional.*

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica. Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo.

Artículo 2. *Del ámbito de actuación y funciones del Centro Criptológico Nacional.*

1. El ámbito de actuación del Centro Criptológico Nacional comprende:

- a) La seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.
- b) La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada.

2. Dentro de dicho ámbito de actuación, el Centro Criptológico Nacional realizará las siguientes funciones:

- a) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.
 - b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.
 - c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.
 - d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.
 - e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.
 - f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.
 - g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.
- Para el desarrollo de estas funciones, el CCN podrá establecer la coordinación oportuna con las comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las tecnologías de la información y de las comunicaciones.

1. Breve introducción

Actividades del CCN

CCN-pytec

¿A qué nos dedicamos?

A PREVENIR



Desarrollo

Art 2. Apdo.2e RD 421/2004: Coordinar la promoción, desarrollo, obtención, adquisición, explotación y uso de tecnologías de seguridad



- › Conocimiento amenazas
- › Necesidades operativas
- › Estado tecnología seguridad
- › Conocimiento industria sector

Evaluación

Art 2. Apdo.2d RD 421/2004: Valorar y acreditar capacidades de productos de cifra para manejar información de forma segura



- › Seguridad funcional
- › Criptológica
- › TEMPEST

Certificación

Art 2. Apdo.2c RD 421/2004: Constituir el organismo de certificación del Esquema Nacional de Evaluación y Certificación del ámbito STIC



- › Seguridad funcional
- › Criptológica
- › TEMPEST



2. Los inicios

CCN ha impulsado el desarrollo de equipos de cifra desde sus orígenes

- Certificados por el CCN
- Empleo en sistemas clasificados
- Sistemas con limitada interconexión a través de redes públicas
- Muchos otros elementos de seguridad (algunos desconocidos) en los sistemas

También se han desarrollado productos específicos para seguridad de las TI

¿Y los sistemas no clasificados?



Epicom



tecnobit grupo oesa



CCN



Epicom

MICROELECTRONICA ESPAÑOLA, S.A.

RECOVERY LABS®

CCN

2. Los inicios

El RD 421/2004, que regula el CCN, crea el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TI

- Inicio actividades relacionadas con la certificación funcional
- Búsqueda de productos con garantías de seguridad
- Sistemas clasificados
 - Productos con certificaciones del CCN (cripto y funcional)



La Administración empieza a interconectarse con el ciudadano

- ¿Qué ocurre con estos sistemas?



3. La evolución

Visión del CCN en relación con los productos de seguridad de las TIC (STIC)

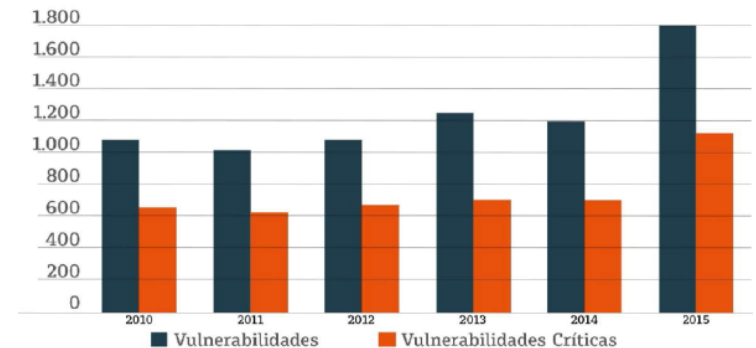
Necesidad de disponer de productos confiables

- Desarrollo de soluciones propias (para **nivel alto de seguridad**)
- Uso de tecnología de seguridad verificada y con garantías

Existe una demostrada incapacidad de los fabricantes para desarrollar aplicaciones carentes de vulnerabilidades

Proceso verificación productos STIC

- Esquema nacional evaluación y certificación productos seguridad (ENECSTI)
- Metodología evaluación funcional (CC y LINCE) y cripto
- Catálogo de Productos CPSTIC (productos aprobados para proteger info Clasificada y cualificados)



3. La evolución

En 2010 se publica el Real Decreto 3/2010, que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y tiene claro cuestión seguridad productos ...

[RD 3/2010, de 8 de enero](#), modificado por [RD 951/2015, de 23 de octubre](#)

Art 18:

“En la **adquisición de productos de seguridad** de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan **certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición**, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.”

3. La evolución

El ENS lo tiene claro ...

[RD 3/2010, de 8 de enero](#), modificado por [RD 951/2015, de 23 de octubre](#)

Medidas Anexo 2: “Componentes certificados [op.pl.5]”

Categoría ALTA

*Se utilizarán **sistemas, productos o equipos** cuyas funcionalidades de seguridad y su nivel hayan sido **evaluados conforme a normas europeas o internacionales** y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.*

Parece que esto mejora ... (al menos desde punto de vista legal)

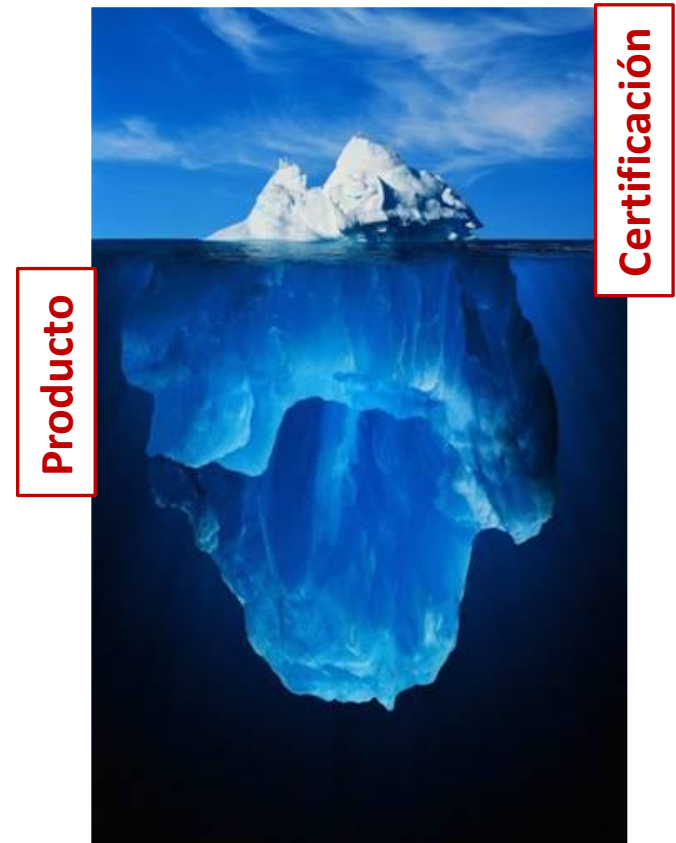
3. La evolución

Pero los productos se certifican contra una Declaración de Seguridad que debe ser...



OJO: ¡La DS la elabora el fabricante!

- ✓ Completa.
- ✓ Consistente.
- ✓ Técnicamente adecuada.

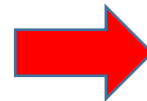


Muchas veces, la Declaración de Seguridad no cubre todos los aspectos de seguridad del producto !!!!

3. La evolución

Comenzamos a elaborar una taxonomía

- Definición de Categorías y familias
- Misma familia – mismos requisitos



Protección de interconexiones

- Enrutadores
- Cortafuegos
- Pasarelas de intercambio de datos
- ...



Confidencialidad e integridad de la información

- Equipos de cifra.
- Herramientas de borrado seguro
- Dispositivos para gestión de claves
- ...



Identificación, autenticación y control de acceso

- Dispositivos biométricos
- Tarjetas inteligentes
- Dispositivos de firma electrónica
- ...



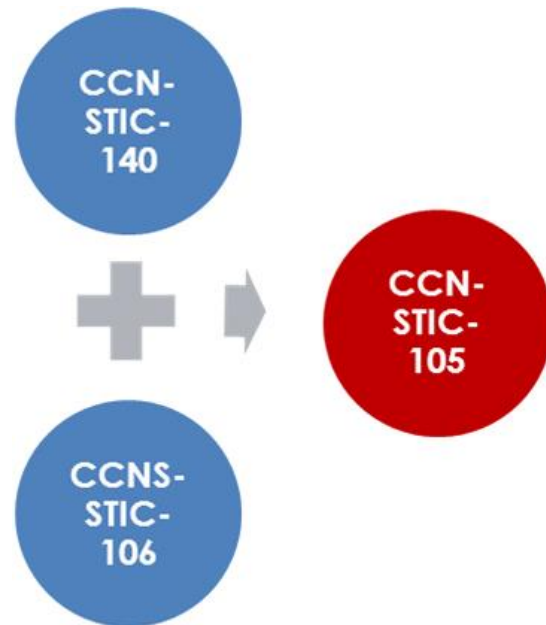
3. La evolución

CPSTIC

<https://www.ccn.cni.es/index.php/menu-pytec-es/productos-de-seguridad-de-las-tic>

Catálogo de Productos para Seguridad de las TIC (CPSTIC)

- Preparación normativa (CCN-STIC-106 y CCN-STIC-140)
- Elaboración requisitos fundamentales seguridad (RFS)
- Análisis inicial posibles productos candidatos
- Publicación inicial del CPSTIC en **diciembre 2017**



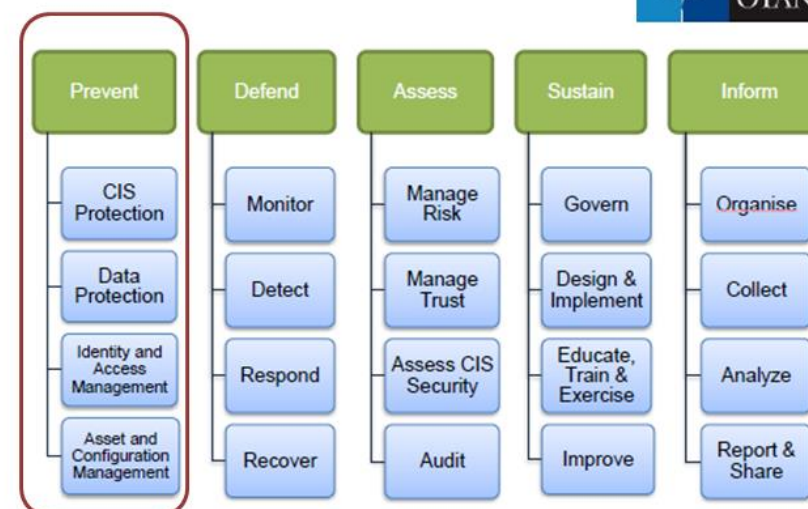
4. La actualidad. Nuevos desarrollos

El CCN continua impulsando el desarrollo de nuevos productos de cifra, tanto para protección información clasificada como para aquella que normativamente requiera protección (ENS), así como otras iniciativas para disponer de productos con garantías de seguridad

- Objetivo fundamental: Generar confianza (en productos de seguridad)
- Necesidad de prevenir y de desplegar soluciones adecuadas



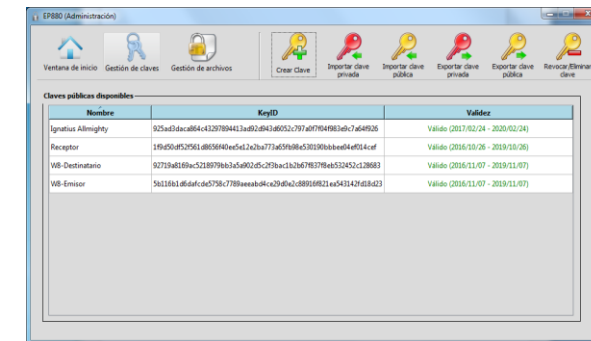
CIS Security (inc. CyberDefence) Capability Breakdown



4. La actualidad. Nuevos desarrollos

Desarrollo de nuevos productos de cifra (ENS alto)

- Nueva generación de cifradores IP (nivel básico de seguridad, tanto personales como de alta velocidad)
- Aplicaciones para seguridad comunicaciones móviles
- Terminales móviles seguros y plataformas confiables
- Software de cifrado de ficheros (CdC)
- Software de cifrado discos duros (nacionalización)



Otros productos STIC

- Intercambio seguro información (nueva generación de pasarelas o adaptación soluciones actuales a entornos específicos)



CRYHOD
FOR DISKS AND LAPTOPS

4. La actualidad. CPSTIC

La Administración lo tiene más fácil para disponer soluciones adecuadas

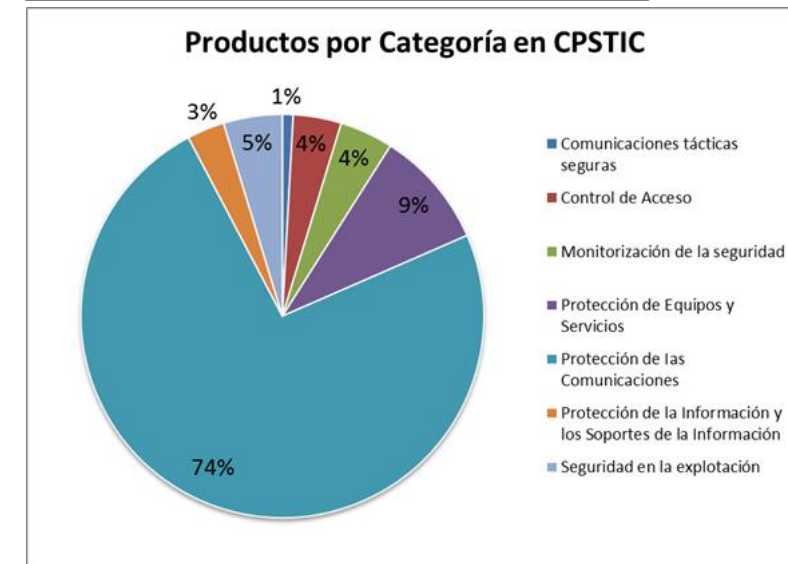
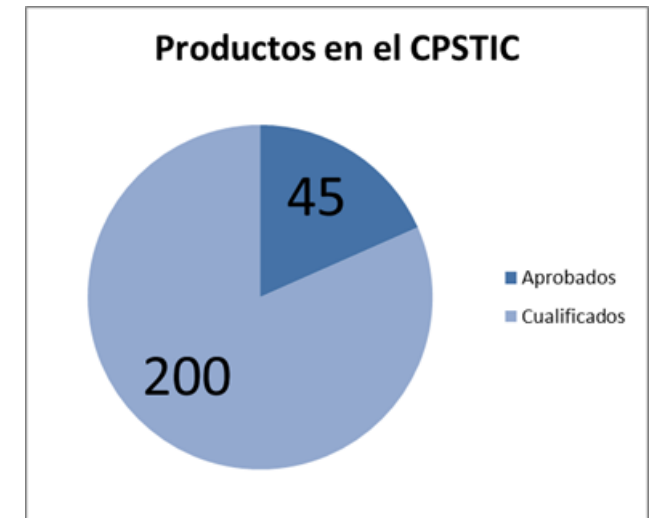
- Productos incluidos en CPSTIC cumplen requisitos seguridad ENS (Cualificados) y para protección información clasificada (Aprobados)



4. La actualidad. CPSTIC

Los fabricantes también lo empiezan a tener claro

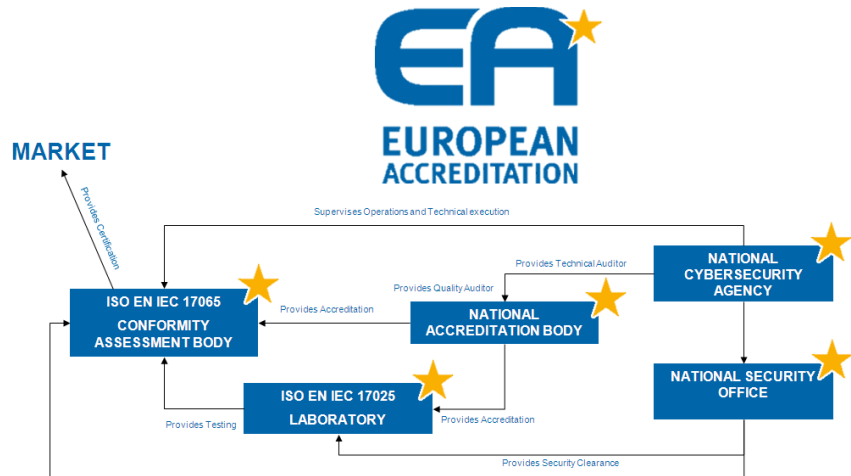
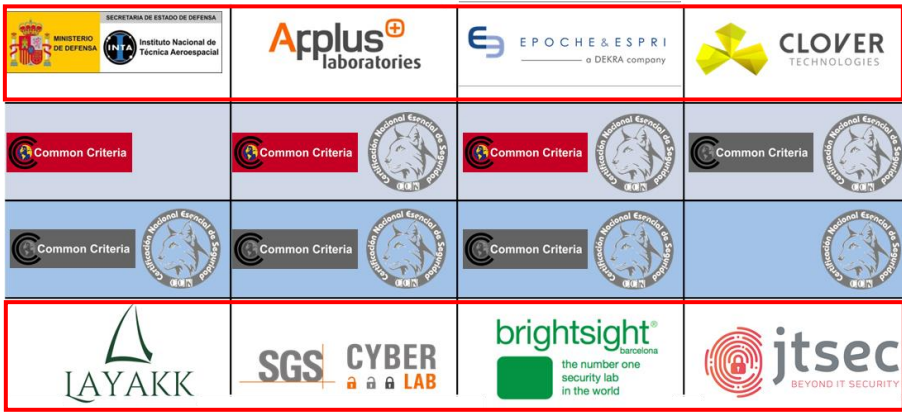
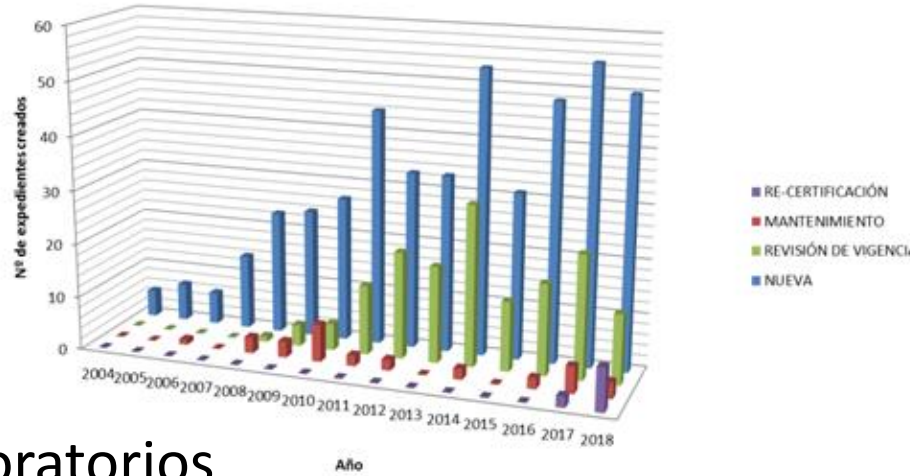
- Quieren estar en el CPSTIC
- Trabajan por conseguirlo
 - Declaraciones de Seguridad más completas
 - Con los RFS de la familia incluidos
 - Interés empresas por estar en CPSTIC
- **Beneficios**
 - Productos con mayores garantías de seguridad
 - Posibilidad de contratación en la Administración
 - Buena tarjeta de presentación para integradores y empresa privada



4. La actualidad. CPSTIC

Los laboratorios también lo tienen claro

- Incremento del numero de certificaciones
- Incremento de solicitudes para acreditación de laboratorios
 - Common Criteria (ISO IEC 15408)
 - Certificación Nacional Esencial Seguridad (LINCE)
- **Cyber Security Act**
 - Europa parece seguir el mismo camino



4. La actualidad

LABORATORIOS DEL ENECSTI



Acreditados ...



En proceso de acreditación ...



4. La actualidad

LABORATORIOS DEL ENECSTI



Acreditados ...



En proceso de acreditación ...



5. Agradecimientos

Agradecimiento a la Administración

- Incluir requisitos de certificación en los pliegos.
- Por tomar el CPSTIC como referencia.
- Por trabajar por conseguir sistemas más seguros.



Agradecimiento a integradores y fabricantes

- Por trabajar por productos/sistemas más seguros.
- Por querer estar en el CPSTIC.



6. Consideraciones finales



6. Consideraciones finales



Necesidad de emplear tecnología de seguridad verificada

- Existencia catálogo productos de seguridad verificados y con garantías (CPSTIC)
- Posibilidad adquirir productos del catálogo para su despliegue
 - Productos CPSTIC adecuados para nivel alto del ENS (cualificados), así como para protección de información clasificada (aprobados)
 - Requisitos Fundamentales Seguridad cubren completamente aspectos de seguridad

Interés y cooperación por parte de los fabricantes

- Muy buena acogida del CPSTIC

Importante esfuerzo para el CCN (compromiso con seguridad productos)

CN-pytec



Muchas gracias



CCN-pytec



OC-CCN

