Cómo mantener tu producto en el catálogo CPSTIC

II
ENCUENTRO
DEL ENS

DIEZ AÑOS DE NUEVOS
RETOS Y SOLUCIONES

CCN
centro criptológico nacional

En colaboración con:

FEMP
FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Índice

1. Panda y jtsec, una relación cibersegura
2. Catálogo CPSTIC: definición, ventajas y acceso
3. Procedimiento de inclusión
4. ¿Un trámite burocrático?
5. Caso de éxito: Panda Security
6. Recomendaciones

Panda y jtsec, una relación cibersegura

- **Javier Tallón:**
- Co-Foundador & Director técnico
- Full-stack ~~hacker~~ wannabe
- Experto en Common Criteria, PCI-PTS, FIPS 140-2, ISO 27K1, SOC2
- Profesor de Ciberseguridad en la Universidad de Granada
- Miembro del grupo de trabajo en certificación de producto de la Agencia de Ciberseguridad Europea (ENISA)

jtsec
BEYOND IT SECURITY

- **Servicios**
  - Laboratorio acreditado evaluación **LINCE**
  - Consultoría Common Criteria, FIPS 140-2 y PCI-PTS
  - Hacking ético
- **Valores**
  - Excelencia técnica
  - Orientación al cliente
  - Tiempo de comercialización

Panda y jtsec, una relación cibersegura

- **Josu Franco:**
- Asesor en Estrategia y Tecnología

- **Servicios**
  - Soluciones de seguridad para endpoint.
  - Mayor fabricante de software empaquetado en España.
  - Recientemente adquirida por Watchguard Technologies.
  - Transición hacia mercado corporativo, AA.PP y gran cuenta. Marca Cytomic.

Catálogo CPSTIC: definición, ventajas y acceso

Art 18 Real Decreto 3/2010 por el que se regula el Esquema Nacional de Seguridad:

*"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."*

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.*

Catálogo CPSTIC: definición, ventajas y acceso

- Metodología ligera
- Sólo válida en España
- Estándar sencillo orientado al análisis de vulnerabilidades y test de penetración
- Duración y esfuerzo acotados
- Más viable económicamente
- Accesible a PYMEs
- Su uso principal es la entrada en el catálogo.

Nivel medio – bajo ENS

Security Target

- Metodología pesada
- Reconocida en 31 países
- Distintos niveles de garantía
- Versátil - Aplicable a todo tipo de productos
- Dificultad técnica para cumplir/entender el estándar.
- Mayor tiempo para su obtención
- Mayor coste económico
- Creada para grandes empresas o productos del sector defensa/banca

Nivel alto ENS

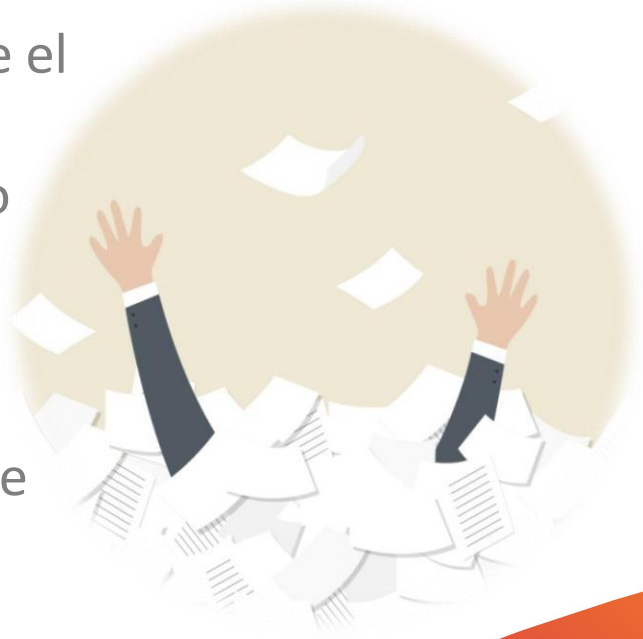
Catálogo CPSTIC: definición, ventajas y acceso

PROBLEMA:

- Los responsables de los sistemas no saben cuáles son los productos certificados *"reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información"*

- La declaración de seguridad la escribe el fabricante, así que podría darse el caso de que la certificación no incluya todas las funcionalidades de seguridad consideradas necesarias por el CCN para un determinado tipo de producto.
    - Hay que leerla para saber el alcance → hay que entender CC

- Si el responsable de los sistemas de cada administración tiene que leerse todas las Declaraciones de Seguridad para una tipología de producto estamos escalando mal. Muy mal.

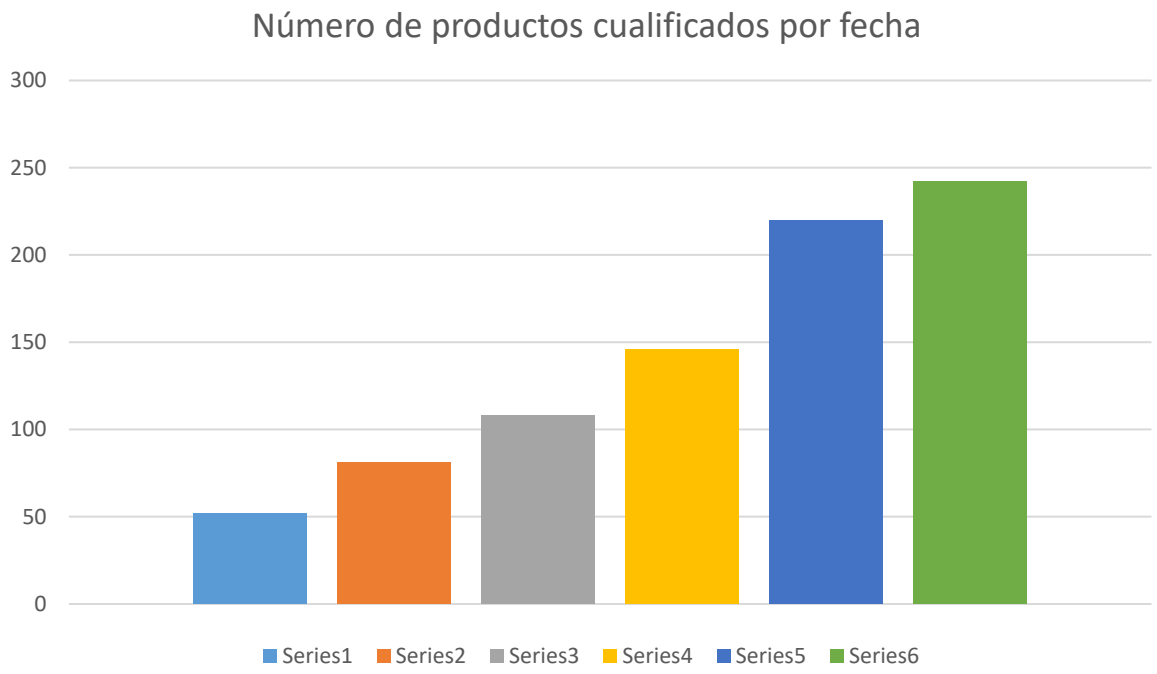


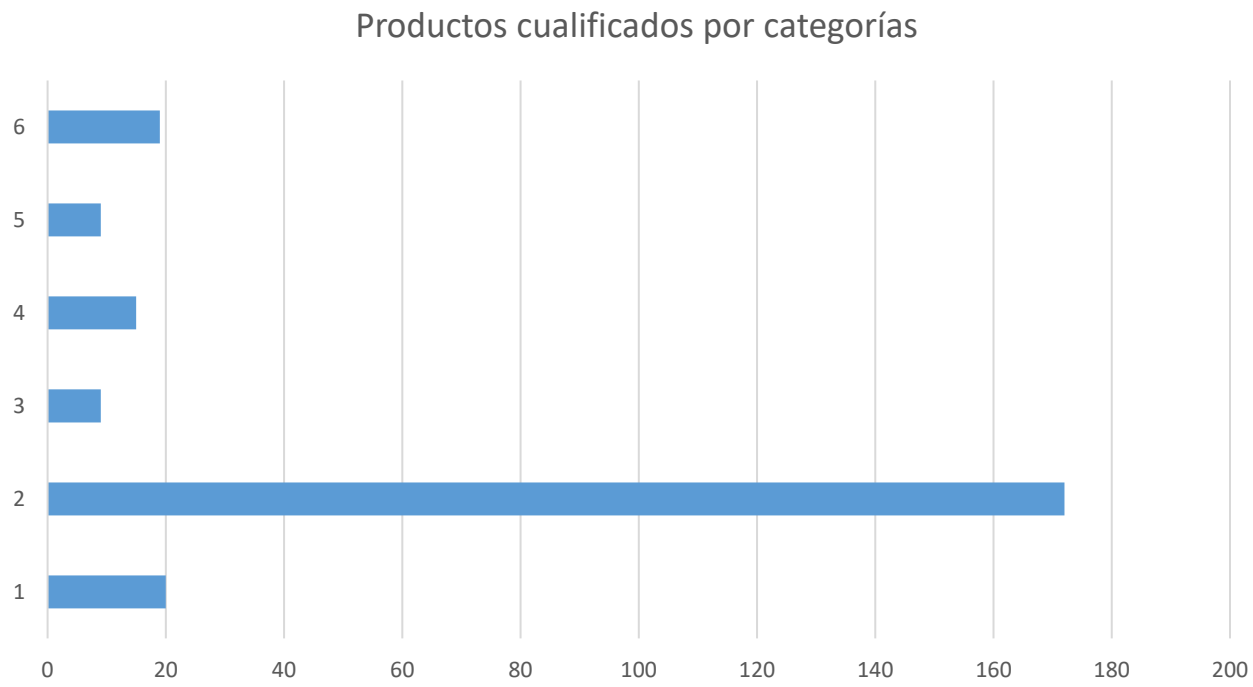
Catálogo CPSTIC: definición, ventajas y acceso

SOLUCIÓN: El catálogo de Productos de Seguridad TIC (CPSTIC) ofrece un listado de productos con unas garantías de seguridad contrastadas por el Centro Criptológico Nacional (ellos validan la ST). Este catálogo incluye los productos **aprobados** para manejar información nacional clasificada y los productos **cualificados** de seguridad TIC para uso en el ENS (CCN-STIC-105). Actualmente existen 7 categorías y 47 familias en su taxonomía de referencia (CCN-STIC-140).

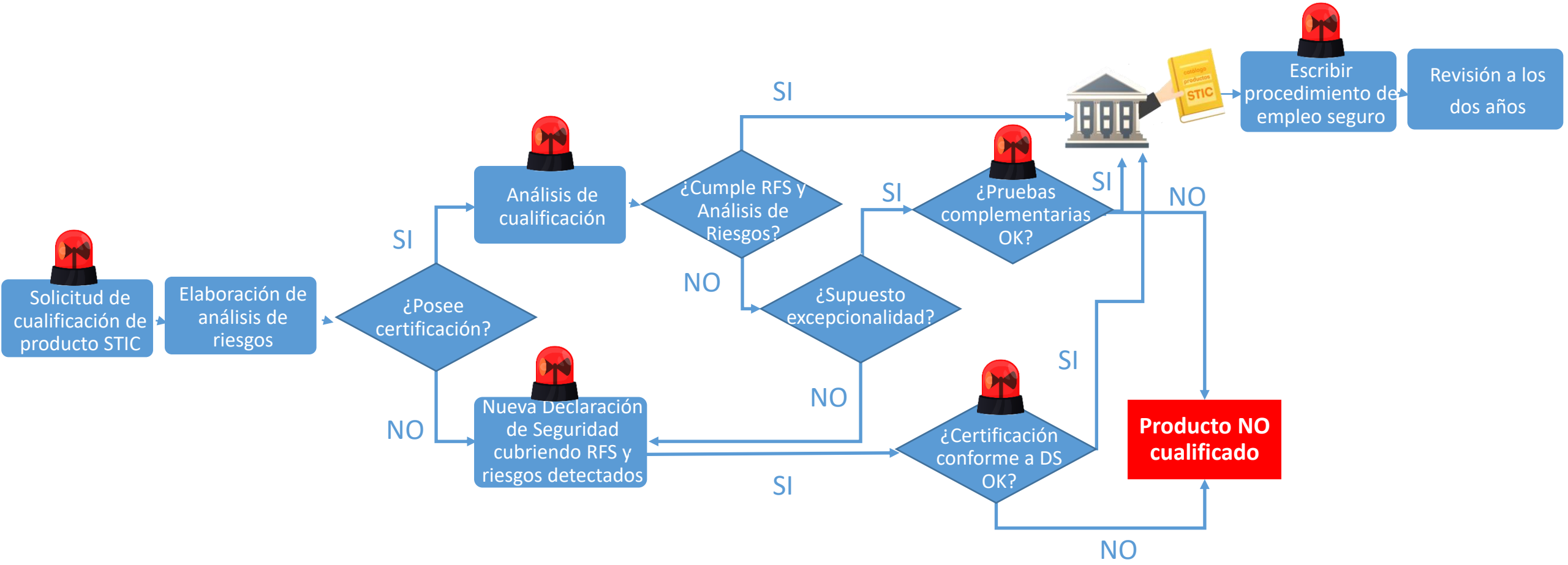
- Ventajas
  - Fácil adquisición de productos ciberseguros
  - Evaluados por parte de un tercero confiable
  - Disponible para todo el mundo

Catálogo CPSTIC: definición, ventajas y acceso





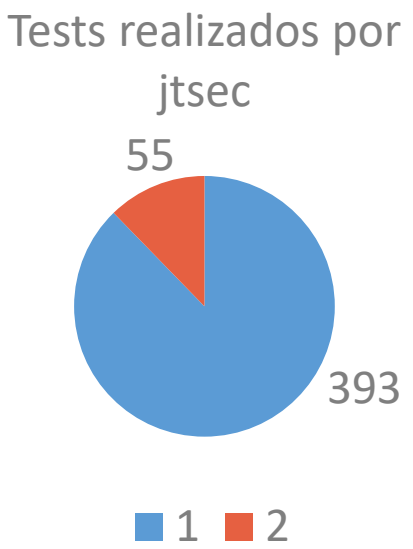
Procedimiento de inclusión

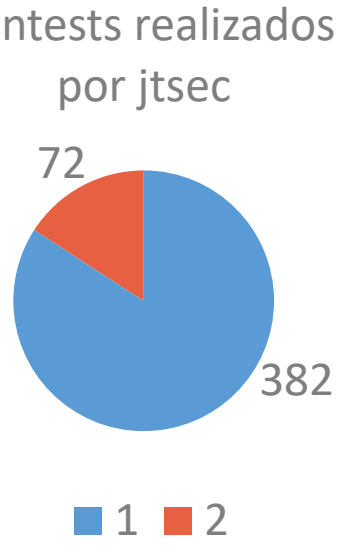


* Simplificado desde CCN-STIC-106 y CCN-STIC-102

¿Un trámite burocrático?

Número de productos evaluados por jtsec	14
Número de tests	448
Número de tests que fallan	55 (12%)
Número de pentests	454
Número de pentests que fallan	72 (16%)



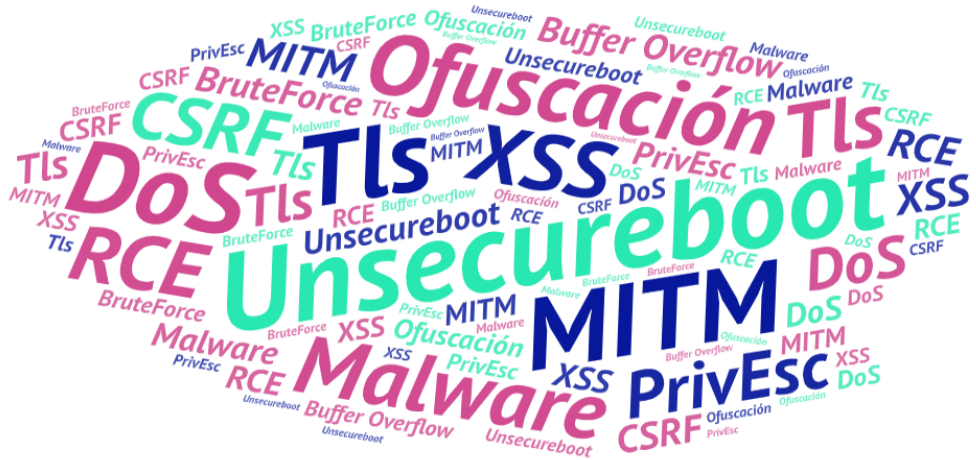


Problemas de cumplimiento

- Uso de mecanismos de cifrado o versiones de TLS no admitidas por CCN-STIC-807

- Identificación incorrecta de bibliotecas de terceros

Vulnerabilidades



Caso de éxito: Panda Security

- Transición hacia segmentos medio y alto del mercado Corporativo.
- Cronología:
  - 2010: primera evaluación de certificación CC. Desechado (coste, tiempo, esfuerzo).
  - 2016: segunda evaluación. Inicio del proceso.
  - Nov. 2016 - Abril 2018:
    - Contratación de asesoría externa.
    - Comienzo de pruebas de certificación.
    - Resolución de no conformidades.
  - Abril 2018 – Nov. 2019:
    - Consecución de la certificación.
    - Entrada en el catálogo.
    - Periodo de uso de la certificación.
  - Nov. 2019 – ahora:
    - Revisión.
    - Documentación de cambios y pruebas complementarias

Recomendaciones

- General
  - Valor de la certificación
    - Necesidad de mercado. Mayor demanda de certificación en pliegos.
    - Necesidad de confianza y credibilidad.
    - Necesidad de mejora de la postura de seguridad. Oportunidad de mejora.

- Para fabricantes:
  - Acompañarse de expertos.
  - Integrar la gestión del proyecto de certificación dentro del mismo equipo de diseño y ejecución de desarrollo del producto, no de forma separada. Integrar requerimientos dentro del propio backlog de desarrollo.
  - Mantener buena comunicación, estar atentos a cambios.

- Para compradores y usuarios:
  - Priorizar/Demandar productos cualificados.

- Para organismos:
  - Equilibro verificación-seguridad-velocidad. Los adversarios no se certifican.
  - Homologación europea de productos cualificados.

II ENCUENTRO DEL ENS

DIEZ AÑOS DE NUEVOS RETOS Y SOLUCIONES

centro criptológico nacional

En colaboración con:

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

Muchas gracias.

Estratégicos

Estándar