El Catálogo de Productos de Seguridad TIC (CPSTIC)

Publicación del CPSTIC

El CCN publica el Catálogo de Productos de Seguridad TIC (CPSTIC), que permite ofrecer un listado de productos de Seguridad TIC, con unas garantías de seguridad contrastadas, a organismos del Sector Público o entidades privadas que den servicio a éstos y que se encuentren afectados por el Esquema Nacional de Seguridad (ENS) o manejen información clasificada.

Estructura del catálogo

El Catálogo constará de dos partes:

1. **Productos Cualificados**.
2. **Productos Aprobados**.

¿Qué son productos Cualificados?

Son productos que tienen certificadas sus funcionalidades de seguridad y, por lo tanto, son aptos para ser utilizados en sistemas afectados por el ENS que hayan sido etiquetados como Categoría ALTA por requerir un nivel alto de seguridad en cualquiera de sus dimensiones (Confidencialidad, Disponibilidad, Integridad, Trazabilidad y Autenticidad).

La necesidad de utilizar productos certificados para este tipo de sistemas viene expresada en el RD 2/2010, de 8 de enero, modificado por el RD 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad[1] (Art. 18 y medidas expresadas en el Anexo 2), donde también se indica que es el Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información (ENECSTI), perteneciente al CCN, quien determinará qué tipos de certificaciones se requieren.

Actualmente, el OC del ENECSTI utiliza diversas metodologías para sus certificaciones de seguridad (*Common Criteria*, ITSEC, ISO 19790 e ISO 24759), aunque es la *Common Criteria* la de uso más extendido y generalista y, por lo tanto, la que se ha tomado como metodología base para el CPSTIC.

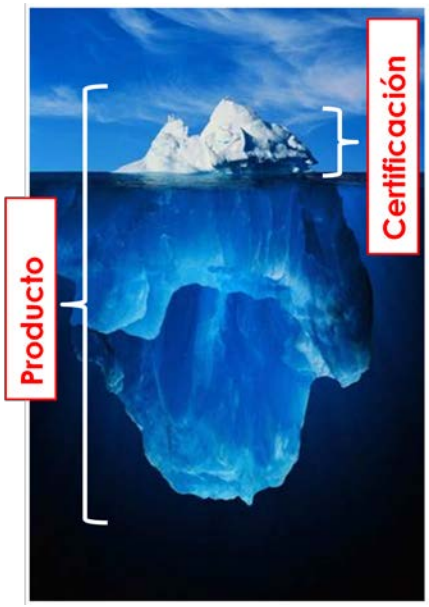
[1] RD 2/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

RD 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

¿Quiere esto decir que un producto Cualificado es lo mismo que uno con Certificación *Common Criteria*?

La respuesta es **NO**, por los motivos que explicamos a continuación.

Que un producto disponga de una certificación funcional *Common Criteria* significa que ha superado con éxito un proceso de evaluación en un laboratorio independiente acreditado, a partir del cual se puede afirmar que su Declaración de Seguridad[2] **es cierta** con un determinado nivel de confianza o "aseguramiento" (EAL[3], en sus siglas en inglés).



Es decir, que durante el proceso de evaluación y posterior certificación se comprueba que las funcionalidades de seguridad declaradas para el producto se encuentran correctamente implementadas, sin entrar en valoraciones de si éstas son suficientes para que el producto sea considerado seguro para un determinado caso de uso como puede ser el previsto en el ENS.

Partiendo de la base de que la Declaración de Seguridad la elabora el fabricante, 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.

No hay que olvidar que *Common Criteria* aporta una metodología de evaluación, responde al ¿**cómo?** pero no dice nada del **¿qué?**, por ello, cabría preguntarse: **¿qué funcionalidades de seguridad incluyo en mi certificación?**

A lo largo de los últimos meses el CCN ha hecho un notable esfuerzo en contestar a esta pregunta. Partiendo de una taxonomía de productos de seguridad TIC organizados en familias, se ha definido para cada una de ellas un listado con los Requisitos Fundamentales de Seguridad (RFS) que como mínimo debe incluir en su certificación un producto que pertenezca a esta familia para que pueda estar en el CPSTIC. Tanto la taxonomía como los RFS correspondientes a cada familia están incluidos en la guía **CCN-STIC-140**, de reciente publicación.

En resumen, por regla general podemos decir que un Producto Cualificado será aquel que cumpla los siguientes requisitos:

1. Poseer una certificación *Common Criteria* en vigor.
2. Que esta certificación incluya los requisitos definidos por el CCN en la guía CCN-STIC-140 para esta familia de productos.

[2] Documento elaborado por el fabricante que contiene una descripción de las funcionalidades de seguridad del producto o sistema y son objeto de evaluación.
[3] *Evaluation Assurance Level.*

3. Que el fabricante o cualquier organismo del Sector Público interesado en que éste sea incluido en el CPSTIC lo haya solicitado formalmente al CCN (más adelante veremos cómo).

Además, **como medida excepcional**, y en aras de resolver el vacío existente al no disponer de productos certificados para algunas familias, el CCN contempla la posibilidad de cualificar productos que no dispongan de certificación CC o que ésta esté incompleta cuando se cumplan las siguientes condiciones:

1. No existen productos certificados de una determinada familia.
2. No existe un fabricante que promueva la certificación desde el punto de vista técnico y económico.
3. El producto se considera de interés estratégico para la Administración.
4. Ha superado con éxito un proceso de evaluación de seguridad TIC previamente acordado con el CCN.

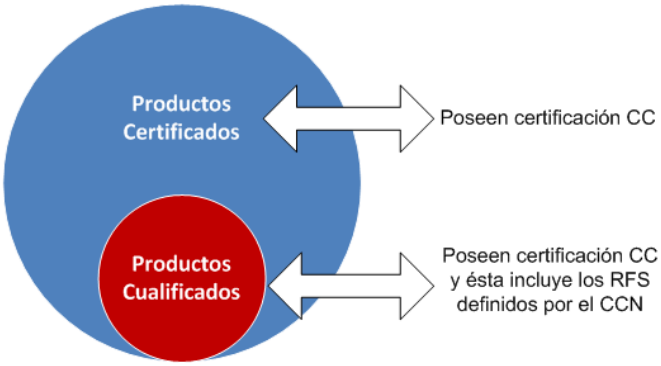


Figura 1 Productos Certificados vs. Productos Cualificados

¿Qué son productos Aprobados?

Son productos cuyo uso está aprobado en sistemas que manejen información clasificada, después de haber superado satisfactoriamente el proceso de aprobación descrito la CCN-STIC-102. En este caso, los productos no sólo cuentan con una certificación funcional conforme a los requisitos descritos en la CCN-STIC-140 para la familia que corresponda, sino que además han superado las evaluaciones adicionales establecidas en la CCN-STIC-102, las cuales dependen del tipo de producto y el grado de clasificación para el que haya sido aprobado. Estas evaluaciones adicionales pueden ser la evaluación criptológica y la evaluación TEMPEST, ambas realizadas por el CCN.

Por lo tanto, como regla general, los productos aprobados están compuestos por un subconjunto de los productos cualificados a los que se le han requerido unas garantías mayores. Adicionalmente, podemos encontrar los productos de cifra que han superado una evaluación criptológica según los requisitos especificados en la CCN-STIC-130, los productos TEMPEST que han

superado una evaluación TEMPEST conforme a la normativa SDIP 27/ 2 (OTAN) o IASG 07-03 (UE), y aquellos armarios apantallados que reducen el riesgo de estas emanaciones y que han sido medidos conforme a la CCN-STIC-153 *"Evaluación y certificación de armarios apantallados"*.

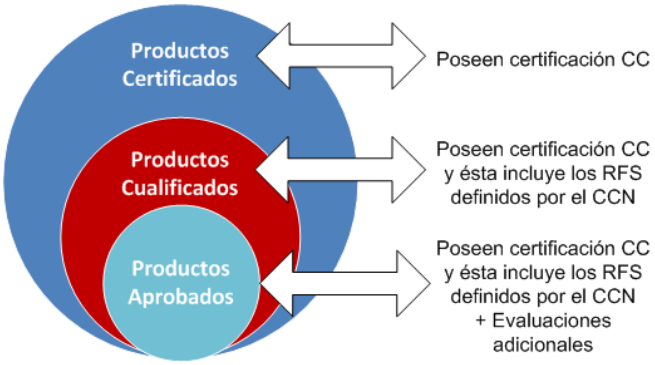


Figura 2 Productos Cualificados vs. Productos Aprobados

Si yo soy un organismo del Sector Público y necesito adquirir un producto TIC para…

1 el ENS, ¿debo recurrir al catálogo?

El uso del CPSTIC no es obligatorio, aunque sí conveniente. Partimos de la base de que la utilización de productos certificados debería estar dentro de los manuales de buenas prácticas a la hora de adquirir tecnología. Básicamente porque han sido evaluados por un laboratorio acreditado para ello, lo que contribuye a la detección y corrección de múltiples vulnerabilidades que incrementan las garantías de seguridad del producto.

Además, como ya hemos adelantado anteriormente, cuando el sistema en que se vaya a utilizar el producto esté afectado por el ENS deberá cumplir con la normativa que lo regula, en la que se establece de manera específica la obligatoriedad de utilizar productos que tengan certificadas las funcionalidades de seguridad relacionadas con el objeto de su adquisición cuando el sistema esté clasificado como Categoría ALTA, y la conveniencia, con carácter general, de utilizarlos para el resto de sistemas.

Por lo tanto, cualquier responsable de la adquisición de productos TIC para un sistema de los expuestos debería no solo comprobar que está certificado, sino que esta certificación es completa, consistente y técnicamente adecuada. Esta es una premisa difícil de cumplir, básicamente por dos motivos:

1. Salvo casos excepcionales, estos responsables no suelen estar familiarizados con la terminología Common Criteria.

2. Es inviable, salvo que se dedique un esfuerzo considerable, tener un conocimiento profundo de las implementaciones concretas de la amplia gama de productos TIC actualmente en el mercado, cuanto más decidir qué requisitos deben exigírsele.

Por todo ello, con el desarrollo del CPSTIC se cumple una doble función:

1. La de realizar esta labor de análisis de certificaciones y discriminar así las que son adecuadas y cumplen los requisitos definidos para esa familia de productos.
2. La de homogeneizar los criterios a la hora de definir qué funcionalidades debe implementar mi producto.

2 un sistema clasificado ¿Qué catálogo empleo?

En el caso de que el sistema maneje información nacional clasificada, se podrán emplear los productos publicados en el apartado de productos aprobados del CPSTIC, la guía CCN-STIC 103 "Catálogo de productos con certificación criptológica" y la guía CCN-STIC 104 "Catálogo de productos con certificación ZONING".

Si no existe un producto en estos catálogos que se adecue a las necesidades del sistema, se deberá solicitar autorización escrita al CCN expresando el producto que se quiere emplear y justificando dicha necesidad.

¿Qué relación tiene este Catálogo de productos con el de Contratación Centralizada del Ministerio de Hacienda y Función Pública?

No tienen ninguna relación, no son excluyentes y podrían utilizarse conjuntamente cuando así lo requiriesen los procedimientos administrativos de adquisición de productos.

El CPSTIC es un catálogo de seguridad meramente técnico que recoge una serie de productos que ofrecen ciertos niveles de garantías para ser utilizados en sistemas que manejan información sensible o clasificada, mientras que el de Contratación Centralizada es un catálogo administrativo desarrollado en base a una serie de convenios marcos negociados con empresas con el objetivo de obtener mejoras de contratación y homogeneización de los niveles de calidad de los servicios y suministros adquiridos por la AGE.

Soy fabricante, tengo un producto certificado y me gustaría incluirlo en el CPSTIC, ¿qué puedo hacer?

En la web del Organismo de Certificación del CCN (https://oc.ccn.cni.es) se encuentra el ***"Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC"*** (CCN-STIC-106), donde se realiza una descripción detallada de los pasos que debe dar un fabricante para que un producto de seguridad TIC sea incluido en el catálogo.

Contacto

ITSEC itsec.ccn@cni.es
ORGANISMO DE CERTIFICACIÓN organismo.certificacion@cni.es