Catálogo de Productos STIC (CPSTIC): regulando la adquisición de productos IT en la administración

El CPSTIC es el catálogo de referencia para la adquisición de productos TIC en organismo públicos afectados por el Esquema Nacional de Seguridad (ENS) y de obligado cumplimiento para la adquisición de productos en organismos que manejen información clasificada. Ha sido diseñado siguiendo una aproximación muy innovadora y que aporta gran flexibilidad para su evolución futura permitiendo la adquisición de productos certificados en la administración española con mayor seguridad y sencillez, y es una herramienta clave que sitúa a España en la vanguardia de la lucha contra las ciberamenazas previniéndolas mediante un adecuado uso de la certificación.

José Ruiz / Javier Tallón

Contexto legislativo: ¿por qué es necesario el catálogo?

La primera pregunta que se viene a la mente es: ¿era necesario crear un catálogo? En primer lugar, conviene contextualizar el marco legislativo alrededor del catálogo.

El CNI es el encargado de velar por la seguridad de las tecnologías de la información en el ámbito de la administración española (Ley 11/2002 de 5 de Mayo). Para ello, se crea dentro de la estructura del CNI el Centro Criptológico Nacional o CCN (RD 421/2004, de 12 de marzo).

Entre las tareas atribuidas al Centro Criptológico Nacional, están las siguientes funciones:

– 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, como las ya conocidas guías CCN-STIC.

– Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, mediante el que siguiendo estándares internacionales como *Common Criteria* (ISO/IEC 15408) y a través de laboratorios acreditados, se certifica la seguridad de todo tipo de productos.

Además, en 2015 se terminó de dar forma al Esquema Nacional de Seguridad (ENS), obligando a cada entidad dentro de la administración (ayuntamientos, diputaciones, universidades…) a seguir ciertas políticas de seguridad en la implantación de sus sistemas de una manera similar a la que proponen otras normas internacionales como ISO 27001, estableciendo para cada administración un nivel de riesgo en función de la criticidad de la información manejada (bajo, medio o alto).

En el ENS se recogen un total de 75 medidas o controles de seguridad que ayudarán a mitigar los riesgos para la seguridad de la información de las administraciones. Entre ellas, para administraciones que manejen información de criticidad nivel ALTO (en algunos casos al nivel medio), se requiere el uso de Componentes Certificados (medida [OP.PL.5]):

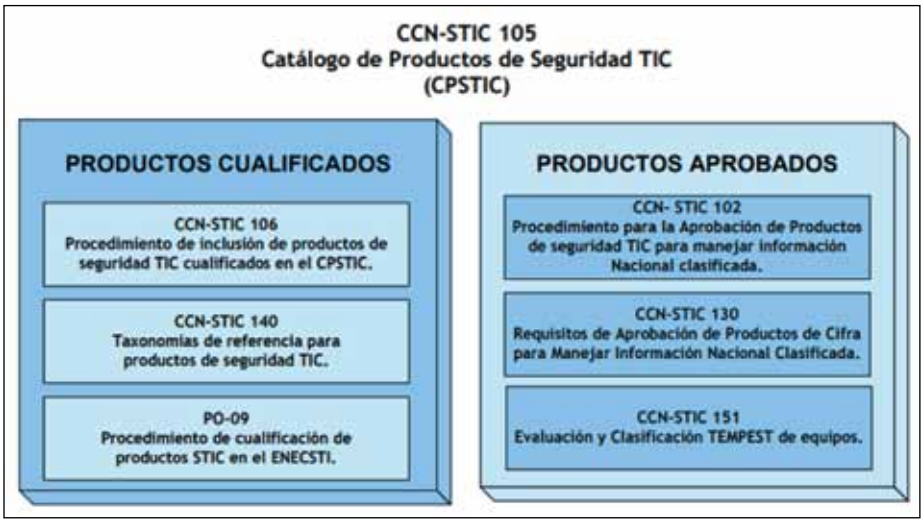

Figura 1

> ***El CPSTIC es un catálogo de referencia para la adquisición de productos TIC en organismo públicos afectados por el ENS y en organismos que manejen información clasificada.***

"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."

Es decir, que si una administración tiene que elegir entre adquirir dos productos de características similares, deberá escoger aquel que esté certificado.

El Artículo 18 del Real Decreto 3/2010 atribuye la responsabilidad de determinar cuáles son los criterios para decidir si un producto está o no certificado al Organismo de Certificación, responsabilidad que ya figuraba de manera genérica entre las que tiene el CCN.

Por lo tanto, el Organismo de Certificación, que está dentro del CCN y que a su vez está dentro del CNI, es el responsable de determinar qué productos deben ser utilizados en la administración para cumplir con el ENS atendiendo a normas europeas o internacionales como ISO/IEC 15408, comúnmente conocida como *Common Criteria*.

¿No es una certificación *Common Criteria* suficiente?

Common Criteria es una certificación de seguridad para productos IT reconocida internacionalmente en virtud de acuerdos internacionales (CCRA) y europeos (SOGIS). El certificado obtenido en España por un fabricante puede usarse en otros países como Francia, EEUU o Alemania y viceversa.

La metodología de evaluación es la más completa que existe actualmente y así se reconoce en el sector. Una certificación *Common Criteria* permite afirmar, con cierto grado de garantía, que un producto cumple con su declaración de Seguridad (DS).

Un problema sobradamente conocido en el sector, es que esta DS es definida por el fabricante y en algunos casos puede no incluir en el alcance de la evaluación una funcionalidad de seguridad que se considere importante para el usuario final (en este caso, la administración española).

La guía CCN-STIC-813, definía de manera general las guías para la adquisición de componentes certificados; sin embargo, esta guía obligaba a cada administración que desease adquirir un producto seguro a revisar todos los productos certificados en todo el mundo, comprobando la Declaración de Seguridad de cada uno para ver si se adaptaba a sus requisitos de seguridad y funcionalidad.

Este problema es solucionado en muchas administraciones de todo el mundo obligando a la certificación de productos que sean conformes a Perfiles de Protección (PP) definidos previamente. Estos PPs son plantillas que determinan la funcionalidad de seguridad a evaluar y el nivel de garantía (EAL) para distintos tipos de productos.

Semejante aproximación es muy costosa en tiempo y recursos, por lo que el CCN optó por una estrategia muy innovadora y que aporta gran flexibilidad de cara al futuro.

¿Qué es el catálogo?

La página web del organismo de certificación perteneciente al CCN (Centro Criptológico Nacional) indica que el Catálogo de Productos STIC (CPSTIC) (guía CCN-STIC 105) ofrece 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.

El Catálogo se compone del Listado de Productos Cualificados: 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).

El Catálogo también incluye el Listado de Productos Aprobados: productos cuyo uso está aprobado en sistemas que manejen información clasificada.

Adicionalmente, el CCN creó la taxonomía (guía CCN-STIC 140), que contiene las diversas categorías de productos que aparecerán en el Catálogo CPSTIC.

En este contexto, una Categoría se define como un tipo de producto de acuerdo a las medidas de seguridad que aporte (p.ej.: control de acceso, protección de las comunicaciones, etc.), coincidiendo éstas con las recogidas en el Anexo II del ENS.

A su vez, para cada Categoría, se han definido diferentes familias de productos, de acuerdo a la funcionalidad principal que implemente (p.ej.: enrutador, cortafuegos, proxy, herramienta de borrado seguro, etc.)

Para cada familia de productos, la taxonomía proporciona un anexo con los requisitos funcionales de seguridad (RFS) que deben cumplir los productos de dicha familia, así como el nivel de evaluación (ej.- EAL 2) requerido. Estos anexos referencian en muchos casos a Perfiles de Protección equivalentes ya definidos, facilitando la inclusión en el catálogo de productos ya certificados bajo la norma Common Criteria.

Por ejemplo, para el caso de la familia "Cortafuegos", dentro de la categoría "Protección de las comunicaciones", el catálogo proporciona diferentes opciones:

– Evaluación conforme a uno de los dos perfiles de protección definidos internacionalmente para este tipo de producto.

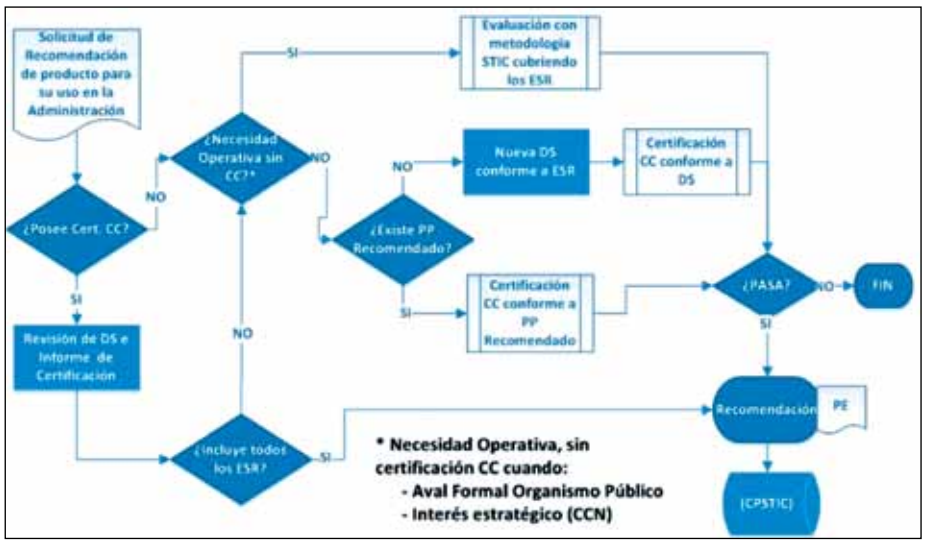

Figura 2

– Evaluación con un nivel de evaluación EAL 2 o superior incluyendo los SFRs listados en los perfiles de protección.

En los casos, en los que no hay ningún perfil de protección conocido, por ejemplo, para la familia "Herramientas de Borrado Seguro" dentro de la categoría "Protección de la Información y Soportes de Información", el catálogo define el nivel de evaluación requerido (EAL 1), indicando los 13 requisitos funcionales de seguridad que deben ser evaluados.

La creación de los anexos para cada familia dota de gran flexibilidad al catálogo puesto que permitirá ampliar/modificar el mismo conforme evolucionen los métodos de evaluación (algo probable con el nuevo marco de certificación promovido a nivel europeo) o se creen nuevos perfiles de protección.

Por último, para que un producto de un determinado fabricante sea incluido en el catálogo como producto aprobado/cualificado se han publicado las guías "Procedimiento para la Aprobación de Productos de Seguridad TIC" (CCN-STIC 102) y "Procedimiento de inclusión de productos de seguridad TIC cualificados en el CPSTIC" (CCN-STIC 106).

Para productos aprobados para el manejo de información clasificada, se requiere la certificación funcional (*Common Criteria*) incluyendo los RFS requeridos en la taxonomía y, si aplica, la certificación Criptológica y Tempest.

Para productos cualificados para uso en la administración conforme al ENS, el solicitante deberá incluir en la solicitud al CCN: la declaración de seguridad (DS), la propuesta de procedimiento de empleo (PE) del producto, el Informe Preliminar de Conformidad de los Requisitos Fundamentales de Seguridad (RFS) y el Listado de algoritmos criptológicos empleados en el producto. La cualificación requerirá la certificación funcional (*Common Criteria*), salvo en casos excepcionales en los que el producto sea considerado de interés estratégico para la Administración y no exista otro similar en el catálogo. En estos casos, el producto puede ser sometido a una evaluación STIC conforme a los Requisitos Funcionales de Seguridad que solicita el anexo por parte de un laboratorio acreditado por el Organismo de Certificación.

Conclusión

El esfuerzo realizado por el CCN permite la adquisición de productos certificados a la administración española con mayor seguridad y sencillez. Así como confirma su apuesta por la certificación para la prevención de los ciberataques.

La creación de un catálogo de productos equipara a España a otros grandes países como EEUU (DoDIN APL) o Reino Unido (CPA), que han utilizado durante años este tipo de herramientas.

El catálogo proporciona una herramienta clave para el futuro de la lucha contra las ciberamenazas. ■

José Ruiz
CTO – Director de Tecnología
jruiz@jtsec.es

Javier Tallón
COO – Director de Operaciones
jtallon@jtsec.es

JTSEC