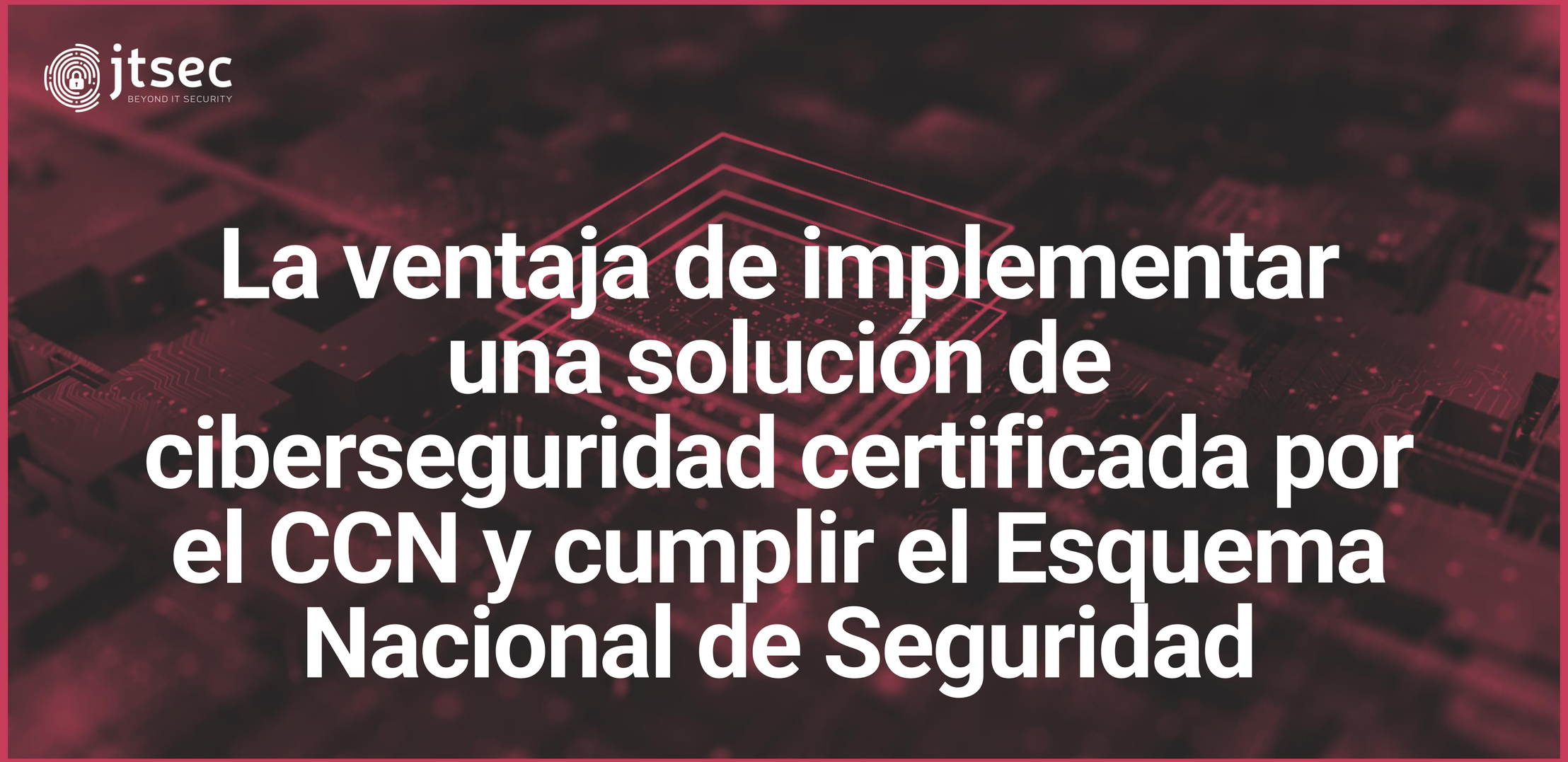

jtsec
BEYOND IT SECURITY
La ventaja de implementar una solución de ciberseguridad certificada por el CCN y cumplir el Esquema Nacional de Seguridad

José Ruiz Gualda

jtsec Beyond IT Security

✉ **jruiz@jtsec.es**

- Ingeniero en Informática (Universidad de Granada)
- Experto en Common Criteria, LINCE y FIPS 140-2 & FIPS 140-3
- Miembro del SCCG (Stakeholder Cybersecurity Certification Group) en la Comisión Europea
- Secretario del SC3 en CTN320
- Editor de LINCE como norma UNE
- Editor en JTC13 WG3 de la Metodología FITCEM
- Editor en el grupo ERNCIP “Certificación de Ciberseguridad IACS” de la Comisión Europea.

jtsec
BEYOND IT SECURITY

jtsec Beyond IT Security

- Laboratorio de Ciberseguridad ofreciendo servicios de auditoria, evaluación y consultoría.
- Primer laboratorio LINCE acreditado por CCN.
- jtsec ha sido premiado con los “Premios SIC 2019” por su contribución con el desarrollo de la metodología LINCE.
- Desarrolladores de una herramienta única en el mercado para la evaluación LINCE, LinceToolBox.
- Ponentes en diferentes eventos del sector como ICCC, ICMC, Jornadas CCN-CERT, EUCA, ENISE, Encuentros UNE…)
- Participantes activos en grupos y actividades de estandarización (CEN/CENELEC, ISCI WGs,ENISA CSA WGs, CCUF, CMUF, ERNCIP)
- Sede en Granada.

INDICE

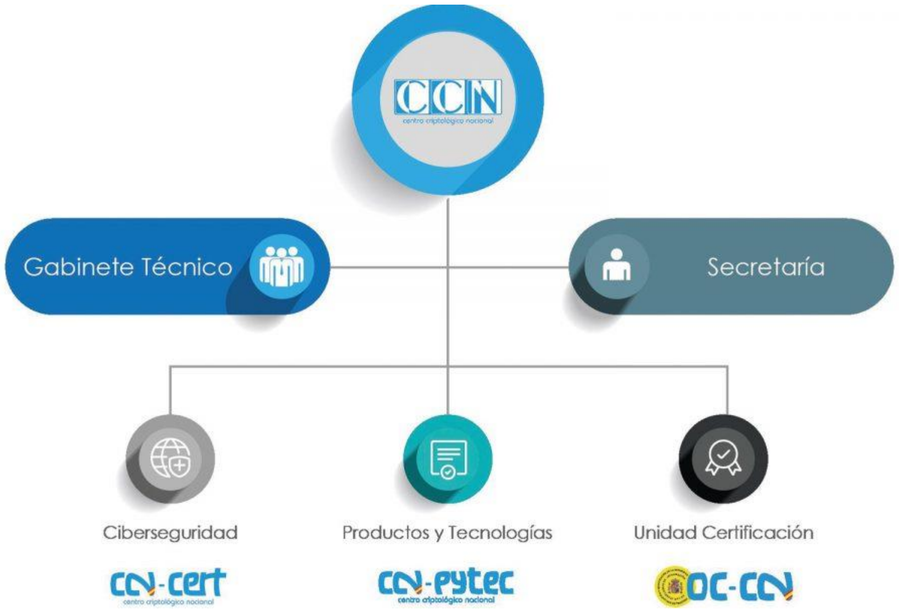
INDICE

Introducción al Centro Criptológico Nacional (CCN) y el Esquema Nacional de Seguridad (ENS).

¿Qué es el CCN?

El Centro Criptológico Nacional (CCN) es el Organismo 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.

El CCN se encuentra dividido en varios departamentos, siendo el CCN-PYTEC el encargado de gestionar el catálogo de producto ciberseguros CPSTIC /CCN STIC-105.



¿Qué es el CCN-PYTEC?

"El Departamento de Productos y Tecnologías del CCN, PYTEC, desempeña las siguientes funciones:

- ✓ Promoción y desarrollo de productos de cifra y seguridad TIC: su objetivo es garantizar que los productos utilizados por la Administración cumplan con los niveles de seguridad exigidos.
- ✓ Evaluación y certificación: La evaluación y certificación de productos de seguridad TIC son el único medio objetivo que permite valorar y acreditar la capacidad de un producto para manejar información segura.
- ✓ Seguridad Productos TIC: el CCN elabora un Catálogo de Productos STIC en el que ofrece un listado de productos de seguridad TIC con unas garantías de seguridad contrastadas por el propio CCN.

Introducción al Centro Criptológico Nacional (CCN) y el Esquema Nacional de Seguridad (ENS).

Contribución CCN a la ciberseguridad en España

Desarrollo de **dos Estrategias de Ciberseguridad Nacional** (2013 y 2019), la implantación del **Esquema Nacional de Seguridad** (ENS), **la creación del CERT Gubernamental Nacional** (CCN-CERT) y la **puesta en marcha del catálogo CPSTIC.**

Además ha colaborado en la **gestión de los ciberataques** en el sector público y en empresas y organizaciones de interés estratégico. El **empleo y promoción de productos y tecnologías de la seguridad**, así como la **formación** de personal experto, la aplicación de políticas y procedimientos, son algunas de las aportaciones más importantes de dicho Organismo.

El CCN y su compromiso con la formación y sensibilización en ciberseguridad

El compromiso de CCN con la sociedad española en el ámbito de la formación y sensibilización de la ciberseguridad se refleja en su amplio **programa de cursos formativos y diversas formas de divulgación** que recopilan los principales consejos que pueden darse a la hora de concienciar y facilitar el uso seguro de las TIC. Dichos cursos están dirigidos al sector privado, al público y a los individuos particulares.

Tal es el éxito que en 2018 se creó una plataforma llamada **Atenea Escuela** para fomentar el uso seguro y conocimiento de las TIC.

Introducción al Centro Criptológico Nacional (CCN) y el Esquema Nacional de Seguridad (ENS).

¿Qué es el ENS?

El Esquema Nacional de Seguridad, de aplicación a todo el Sector Público, así como a los proveedores que colaboran con la Administración, **ofrece un marco común de principios básicos, requisitos y medidas de seguridad** para una protección adecuada de la información tratada y los servicios prestados, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias. Desde su primer desarrollo en 2010 está en constante evolución con modificaciones notables en 2015 y su **última actualización en 2022 (Real Decreto 311/2022**).

Introducción al Centro Criptológico Nacional (CCN) y el Esquema Nacional de Seguridad (ENS).

Extracto Real Decreto 311/2022

Según el ENS, y citando textualmente un extracto del punto 4.1.5 de la mencionada legislación: «Se utilizará el **Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación** (CPSTIC) del CCN, para **seleccionar los productos o servicios suministrados por un tercero** que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las **medidas de este real decreto**».

Conclusión

Se puede concluir del extracto que es **obligatorio contar con una cualificación de ciberseguridad para los productos TIC**. Además, cumplir con la normativa es uno de los criterios de selección que utiliza el sistema dinámico de **adquisición en la Administración Pública.**

INDICE

¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

El catálogo de productos ciberseguros CPSTIC / CCN STIC-105 ofrece un **listado de productos con garantías de seguridad contrastadas por el Centro Criptológico Nacional** (CCN valida el alcance de la evaluación (ST) y las pruebas realizadas). Este catálogo incluye productos aprobados para manejar información clasificada nacional y productos cualificados de seguridad TIC para su uso en el ENS (CCN-STIC-105).**El catálogo está en continuo crecimiento con nuevas taxonomías y soluciones incluidas.**

Taxonomías catálogo CPSTIC

El Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN está en **continua evolución, incluyendo nuevas categorías y familias** debido a la evolución del propio mercado. En algunas ocasiones, los requerimientos son de tipo legal, tal y como sucede con las soluciones de videoidentificación, que, de acuerdo con el BOE núm. 115, de 14 de mayo de 2021, obliga a los prestadores de este tipo de servicios a validar sus soluciones

¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

Estructura catálogo CPSTIC

PRODUCTOS Y SERVICIOS CUALIFICADOS

Cumplen con alguna de las categorías del ENS (básica, media o alta)

Para que un producto o servicio sea cualificado, debe cumplir con los RFS definidos para cada familia, incluidos en los correspondientes anexos de la guía CCN-STIC 140

PRODUCTOS y SERVICIOS APROBADOS

La taxonomía de productos aprobados para el manejo de información clasificada es la misma que para los cualificados junto con las categorías Protección en entornos tácticos y Tempest.
Los RFS son los mismos que los cualificados mas los específicos establecidos en la CCN-STIC-130

SERVICIOS DE CONFORMIDAD Y GOBERNANZA DE LA SEGURIDAD

El acceso a esta categoría no requiere realizar una Declaración de Seguridad y superar una evaluación LINCE, Common Criteria o CPSTIC, pero sí superar unas pruebas de penetración para verificar que la herramienta cumple con unos mínimos de seguridad.

jtsec
BEYOND IT SECURITY

¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

¿Cómo incluir tus productos en el catálogo?

LINCE

Certificación fixed-time (25 días) para niveles de seguridad medio o bajo, de acuerdo con la clasificación del ENS.

Certificación con reconocimiento a nivel nacional, que permite, en un tiempo y esfuerzo acotados obtener una certificación emitida por el CCN, más viable económicamente y accesible a PYMES.

Estándar orientado al análisis de vulnerabilidades y test de penetración. Además, es norma UNE.

Common Criteria

Metodología pesada para niveles de seguridad altos. Reconocida en más de 30 países y consta de diferentes niveles de garantía (EAL1-EAL7).

Permite incluir el producto en el catálogo (mínimo EAL2). Es un estándar difícil técnicamente de cumplir, necesitando mas tiempo/coste obtenerlo

Dependiendo del alcance de la evaluación original es necesaria la realización de pruebas STIC complementarias.

Certificación Nacional Esencial de Seguridad
CCN

COMMON CRITERIA

¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

¿Cómo incluir tus productos en el catálogo?

STIC Complementaria
Se realiza a algunos de los productos que ya han obtenido una certificación Common Criteria y que pretenden formar parte del catálogo CPSTIC.

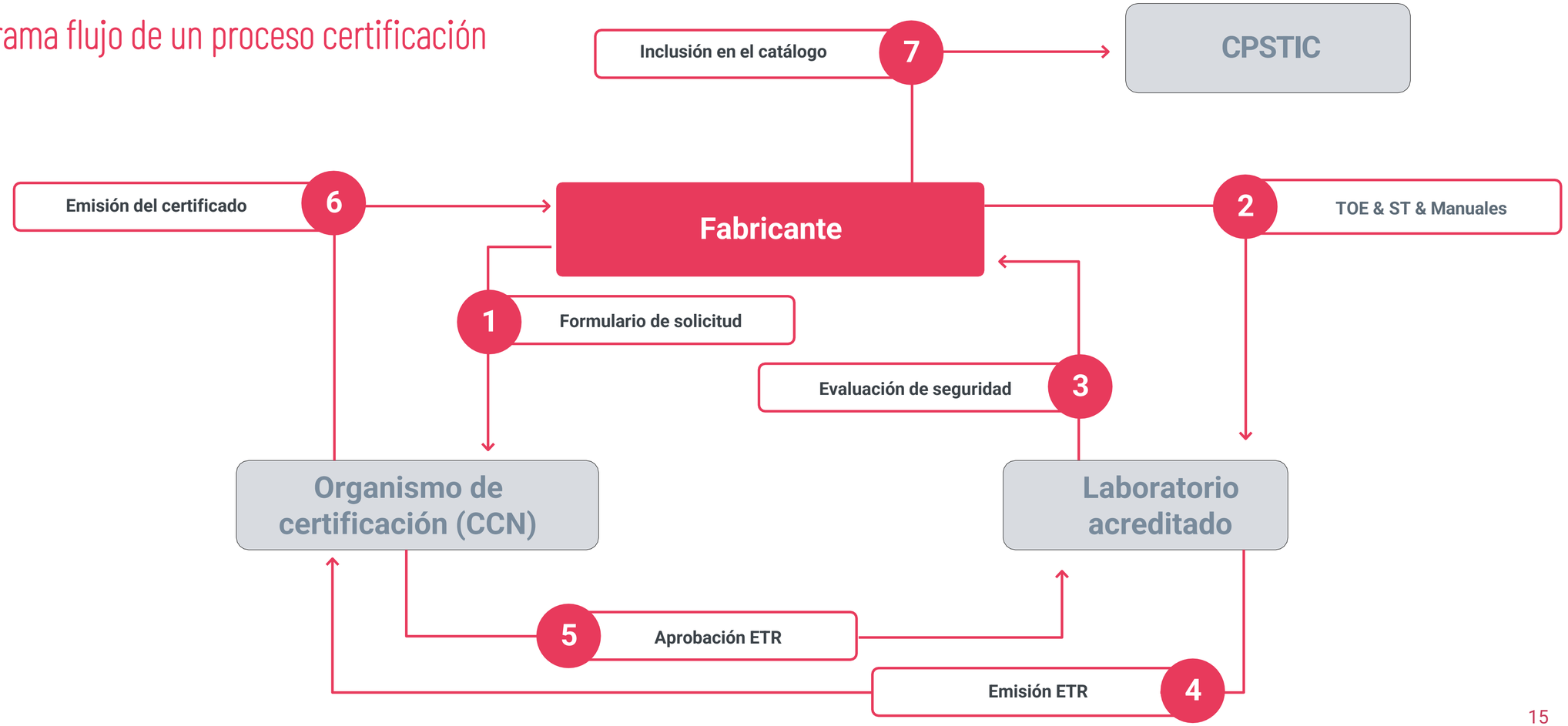
Dependiendo del nivel de seguridad (EAL) obtenido, el producto requiere de la realización de ciertas pruebas STIC complementarias para poder acceder al catálogo.

Evaluación STIC - Nube
Creada para soluciones cloud nativas donde no se puede certificar una versión específica, sino que están en continuo desarrollo.

Además de cumplir con los requisitos especificados para su taxonomía, la solución deberá superar los requisitos especificados en el Anexo G "Servicios en la nube"

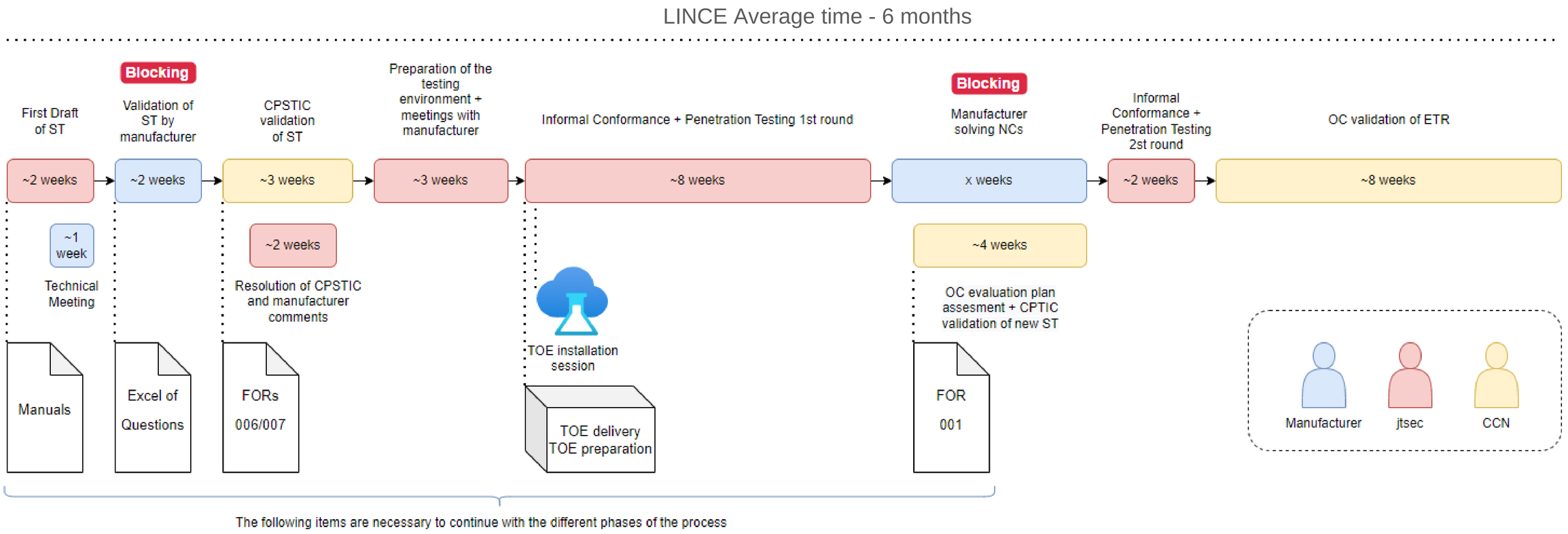
¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

Diagrama flujo de un proceso certificación



¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

Diagrama flujo de trabajo certificación LINCE



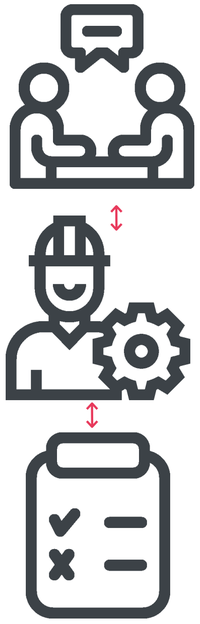
¿Qué es el CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC)?

Equipos que participan en el proceso

FABRICANTE

- Equipo directivo.
- Equipo legal
- Project managers / Equipo Certificación

- Técnicos/Desarrolladores



jtsec

Equipo ventas
Primer contacto, decisiones a alto nivel.

Equipo consultoría
Guía durante el proceso. Genera documentación (ST). Comunicación constante con fabricante, otros equipos jtsec y CCN / CPSTIC.

Equipo evaluación
Realiza las pruebas de seguridad. Genera el Informe de Pruebas de Evaluación (ETR). Independencia crítica.

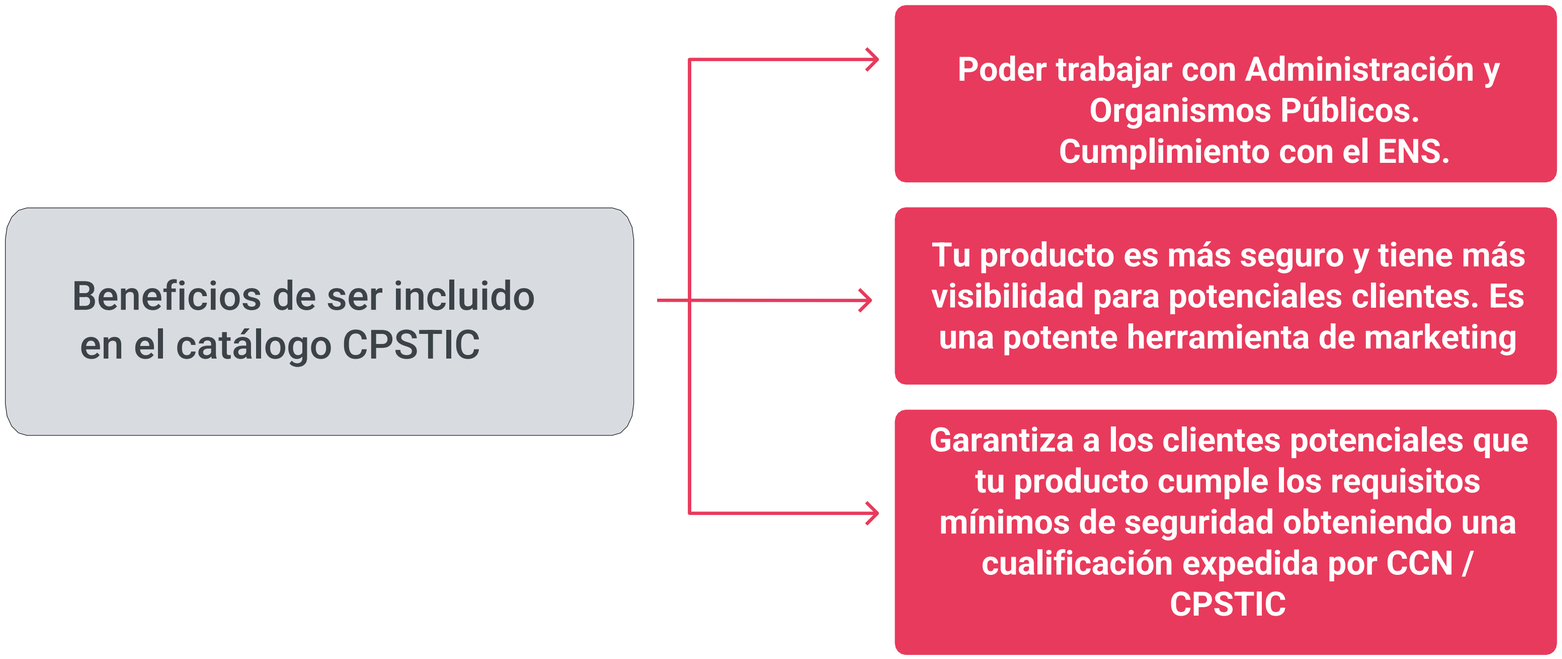
CCN / CPSTIC

Mantiene el catálogo STIC; aprueba el ST y otra documentación. Crea taxonomías, normas...

Aprueba el ETR y eltrabajo de laboratorio.

INDICE

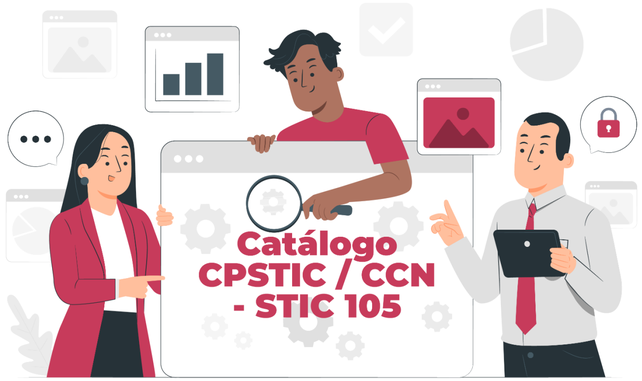
Los beneficios de la certificación por el CCN y el cumplimiento del ENS para tu organización.



Los beneficios de la certificación por el CCN y el cumplimiento del ENS para tu organización.

Adquisición de productos por parte de la Administración

El **sistema dinámico de adquisición** en la Administración Pública es un método electrónico de contratación continua que está abierto a todas las empresas interesadas que cumplan con los criterios de selección.
Estos sistemas dinámicos de adquisición **incorporan condiciones generales para exigir certificaciones/cualificaciones de seguridad**, así como métodos aceptables para demostrar la seguridad, estableciendo conexiones con el ENS, el CPSTIC y las certificaciones que puedan derivar del Reglamento (UE) 2019/881.
El sistema **se compone de dos etapas**.



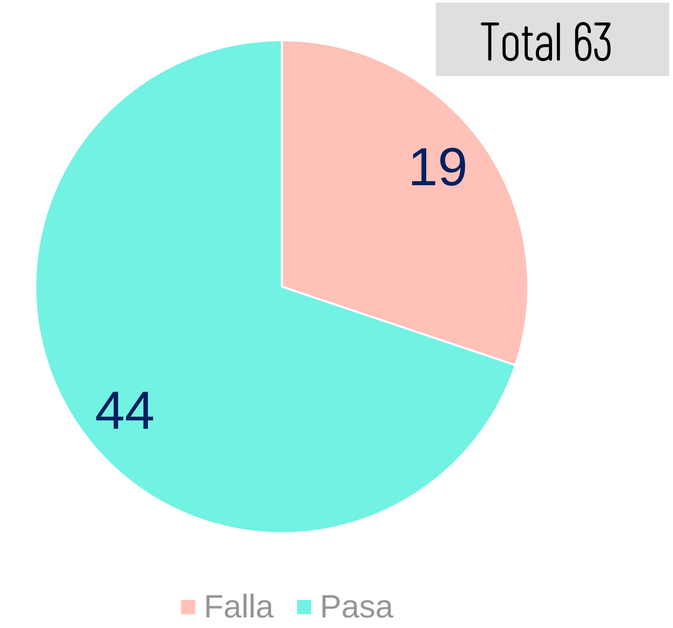
1 Las compañías que cumplen con los criterios de selección necesarios son admitidas en el sistema dinámico de contratación

2 Las corporaciones admitidas en la ronda anterior presentan sus ofertas.

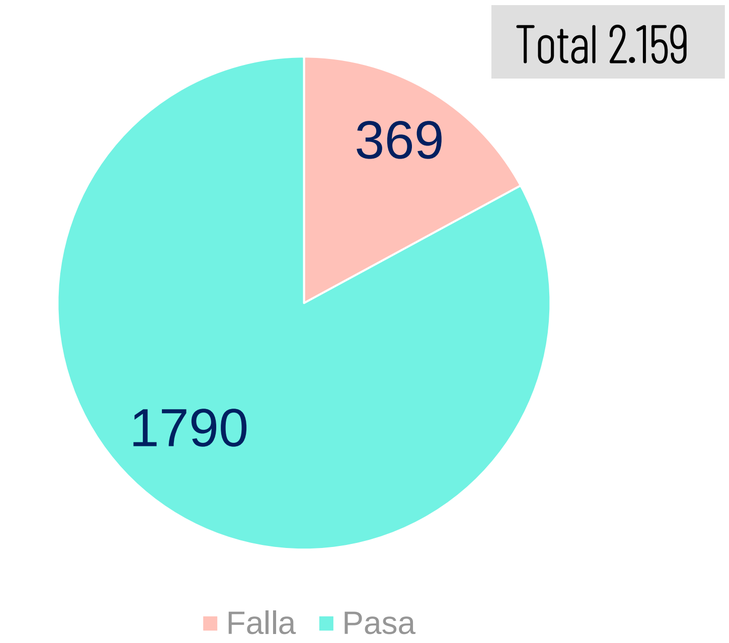
Los beneficios de la certificación por el CCN y el cumplimiento del ENS para tu organización.

Datos sobre proyectos evaluados por jtsec en 2022

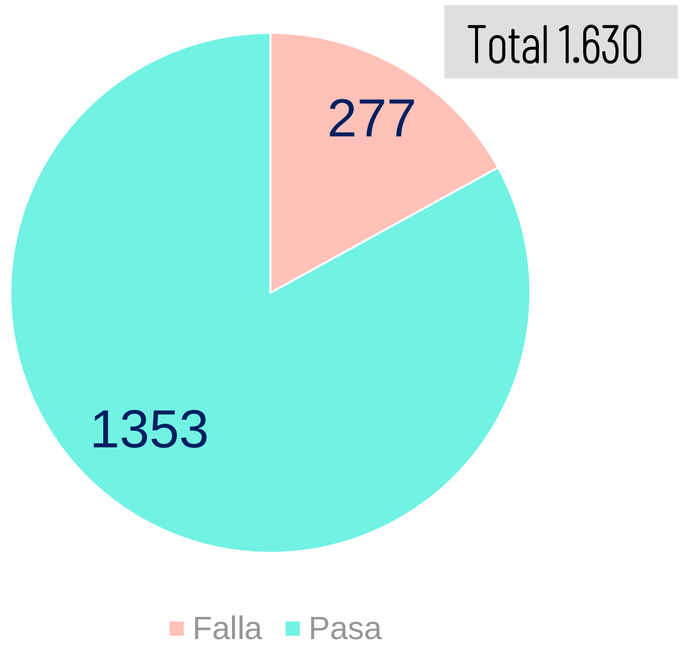
Número de proyectos por resultado en fase de validación



Número de test funcional por resultado en fase de evaluación

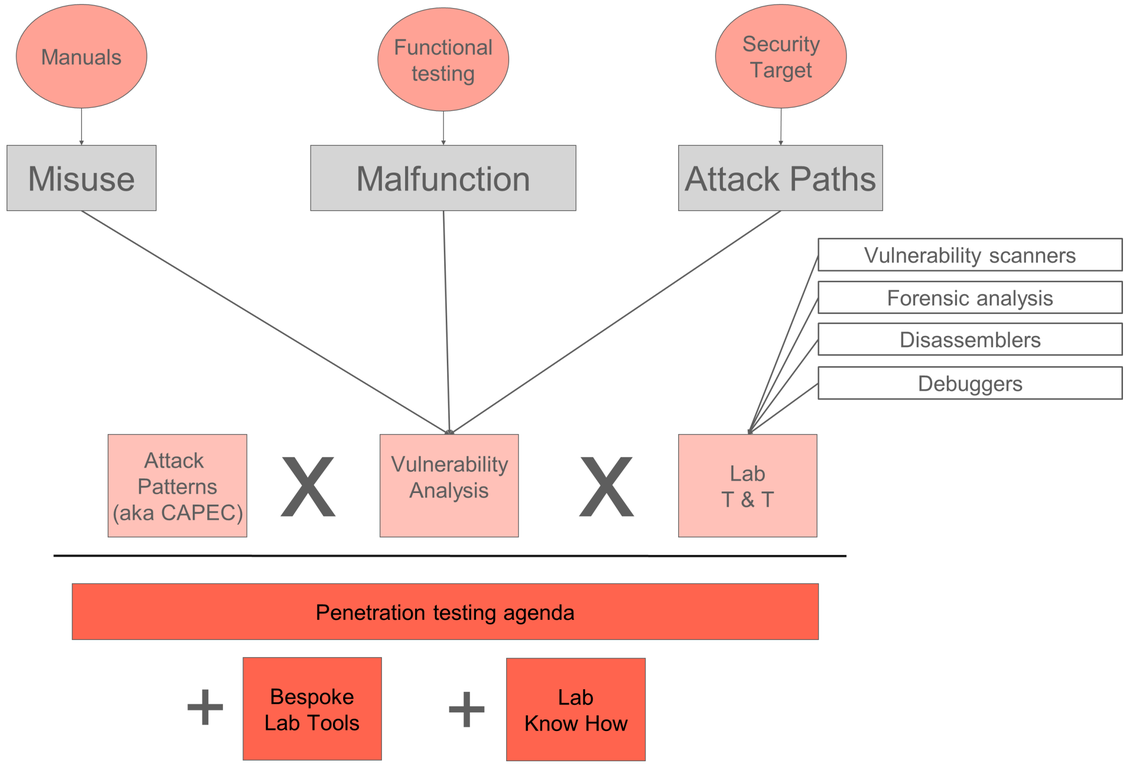


Número de pentest por resultado en fase de evaluación



Los beneficios de la certificación por el CCN y el cumplimiento del ENS para tu organización.

¿Cómo hacer una análisis de vulnerabilidades?



Los beneficios de la certificación por el CCN y el cumplimiento del ENS para tu organización.

Conclusiones

La Administración española está implementando mecanismos, como el CPSTIC, para utilizar y adquirir productos TIC que hayan pasado una evaluación de seguridad y que cuenten con un procedimiento de empleo seguro.

La nueva versión del ENS hace referencia al catálogo CPSTIC incluyéndolo dentro del marco legal. Adicionalmente, tanto a través del sistema dinámico de adquisición como en la redacción de pliegos por parte de las distintas administraciones, vemos el impulso necesario que anime a los fabricantes a seguir invirtiendo en los procesos de certificación/cualificación de sus productos.

El CPSTIC es uno de los pilares para la prevención de los ciberataques


jtsec
BEYOND IT SECURITY
Gracias