

Guía de Seguridad de las TIC

CCN-STIC 2101

Procedimiento de Autorización de Laboratorios para Evaluaciones CCN-STIC 2100 (MEMeC)



Marzo 2025



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025

NIPO: 083-25-212-5.

Fecha de Edición: marzo 2025.



centro criptológico nacional

CENTRO CRIPTOLOGICO
NACIONAL

cn=CENTRO CRIPTOLOGICO
NACIONAL, 2.5.4.97=VATES-
S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO
NACIONAL, c=ES
2026.01.16 12:24:19 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	4
2. OBJETIVO Y ALCANCE	5
3. REQUISITOS DE AUTORIZACIÓN DE LABORATORIOS PARA EVALUACIONES CCN-STIC 2100 (MEMEC)	6
4. PROCESO DE AUTORIZACIÓN DEL CCN.....	7
4.1 SOLICITUD DE AUTORIZACIÓN DEL CCN	7
4.2 VIGENCIA DE LA AUTORIZACIÓN.....	7
4.3 LISTA DE LABORATORIOS AUTORIZADOS	8
5. REFERENCIAS	9
6. ABREVIATURAS	10

1. INTRODUCCIÓN

1. La adquisición de un producto o la contratación de un servicio de seguridad TIC que va a manejar información nacional clasificada o información sensible debe estar precedida de un proceso de comprobación de que los mecanismos de seguridad implementados en el producto o servicio son adecuados para proteger dicha información.
2. La evaluación y certificación de un producto o servicio de seguridad TIC es el único medio objetivo que permite valorar y acreditar su capacidad para manejar información de forma segura. En España, esta responsabilidad está asignada al Centro Criptológico Nacional (CCN) a través del RD 421/2004 de 12 de marzo [REF1] en su Artículo 1 y en su Artículo 2.1, el cual establece que el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y la comunicación y autoridad de certificación criptológica.
3. Basándose en las competencias otorgadas, el CCN publica la guía **CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) [REF2]**. Esta guía permite proporcionar un nivel mínimo de confianza al usuario final en los productos o servicios adquiridos, debido a las mejoras de seguridad derivadas del proceso de evaluación y certificación y a un procedimiento de empleo seguro.
4. Para la inclusión de un producto STIC dentro del catálogo CPSTIC, el CCN establece el **Procedimiento de Cualificación** para productos que vayan a manejar información sensible en el Esquema Nacional de Seguridad (ENS) y el **Procedimiento de Aprobación** para productos destinados a manejar información nacional clasificada. Ambos procedimientos abarcan la evaluación de aspectos relativos a la implementación de los requisitos funcionales de seguridad en dicho producto, así como otros aspectos del producto que aumentan su seguridad y la mantienen a lo largo de la vida útil del mismo.
5. En el caso de que el producto utilice criptografía para proteger la confidencialidad, integridad, autenticidad y/o el no repudio de la información nacional clasificada, también es fundamental abarcar los aspectos relativos a la seguridad criptológica de los algoritmos empleados, tanto los relacionados con su implementación en el equipo o sistema donde se incluyan, como la eficacia de sus mecanismos de autoprotección.
6. Para ello el CCN, con el objetivo de facilitar y estandarizar el trabajo tanto de laboratorios como de fabricantes, establece la metodología de evaluación nacional de mecanismos criptográficos, publicada en la guía **CCN-STIC 2100 Metodología de Evaluación de Mecanismos Criptográficos (MEMeC) [REF3]**. En esta guía se especifican el conjunto de tareas para evaluar las implementaciones criptográficas incluidas en los productos tecnológicos que se deberán realizar durante el proceso de evaluación.

2. OBJETIVO Y ALCANCE

7. Dada la elevada especialización requerida para la realización y validación de las tareas de evaluación, así como la complejidad del equipamiento necesario para la ejecución de determinadas pruebas, es preciso asegurar que los laboratorios poseen unas mínimas capacidades y equipamiento para la aplicación de dicha metodología.
8. El objetivo de este documento es definir los requisitos y el procedimiento que tienen que cumplir los laboratorios para ser autorizados por el CCN para la evaluación de productos conforme a la guía **CCN-STIC 2100 Metodología de Evaluación de Mecanismos Criptográficos (MEMeC) [REF3]** como parte de los procesos de cualificación y aprobación.

3. REQUISITOS DE AUTORIZACIÓN DE LABORATORIOS PARA EVALUACIONES CCN-STIC 2100 (MEMeC)

9. Los laboratorios que evalúen mecanismos criptográficos como parte de los procesos de cualificación y/o aprobación deberán disponer de la condición de **laboratorio autorizado por el CCN** para la realización de evaluaciones CCN-STIC 2100 (MEMeC) en adelante evaluaciones MEMeC.
10. Los requisitos para la obtención y mantenimiento de la condición de laboratorio autorizado son los siguientes:
11. **REQ.1.** Ser un laboratorio acreditado del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) conforme a lo establecido en el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ORDEN PRE/2740/2007) [REF4].
12. **REQ.2.** Realizar una evaluación de prueba, bajo las condiciones y procedimientos de un proceso de cualificación o aprobación, para la demostración de la correcta aplicación de la guía CCN-STIC 2100 Metodología de Evaluación de Mecanismos Criptográficos (MEMeC) [REF3] cuyo nivel de aseguramiento “*Certification Level* (CL)” en terminología MEMeC, sea el de la autorización solicitada.
13. Antes de comenzar la evaluación, el CCN deberá dar el visto bueno tanto al producto, para garantizar que es adecuado para ejercitar la completitud de las pruebas requeridas, como al laboratorio, para asegurar que su capacitación técnica es suficiente para abordar la evaluación.
14. Los resultados de la evaluación no podrán ser utilizados para los correspondientes procesos de cualificación/aprobación del producto que implementa los mecanismos evaluados hasta que el laboratorio obtenga la condición de laboratorio autorizado por parte del CCN.
15. **REQ.3.** Demostrar la capacidad para la evaluación de los mecanismos criptográficos mediante la acreditación de la competencia técnica en vigor, conforme a la norma UNE-EN ISO/IEC 17025 [REF5]. El alcance deberá indicar como producto/material de ensayo los mecanismos criptográficos con un nivel de aseguramiento (CL) igual al de la evaluación de prueba del **REQ.2**, y la norma/procedimiento de ensayo para estos productos deberá ser la guía CCN-STIC-2100 Metodología de evaluación de mecanismos criptográficos (MEMeC) [REF3].
16. La acreditación de competencia técnica, deberá haber sido concedida por la Entidad Nacional de Acreditación (ENAC), organismo nacional de acreditación designado en el Real Decreto 1715/2010, de 17 de diciembre [REF6], de acuerdo con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de Julio de 2008.

4. PROCESO DE AUTORIZACIÓN DEL CCN

4.1 SOLICITUD DE AUTORIZACIÓN DEL CCN

17. Únicamente se contempla la solicitud de la condición de laboratorio autorizado por el CCN para la realización de evaluaciones MEMeC como parte de los procesos de cualificación/aprobación.
18. La solicitud se realizará mediante el formulario “FOR-CRIPTO-01”, disponible en la página web <https://oc.ccn.cni.es>, que deberá ir acompañado de la siguiente documentación:
 - a) La acreditación del laboratorio como laboratorio del ENECSTI.
 - b) El “*Vendor Questionnaire (VQ)*” y, opcionalmente, la documentación adicional del fabricante que complementa la información contenida en el VQ, es decir la entrada “*I1: Cryptographic Mechanisms Evaluation Vendor Questionnaire and, optionally, Vendor Documentation*” de la metodología de evaluación MEMeC [REF3].
 - c) Informe de la capacitación técnica del laboratorio para la realización de las distintas tareas de evaluación especificadas en la CCN-STIC 2100 (MEMeC) definidas en términos: formación del personal, experiencia, asistencia a eventos, jornadas técnicas, participación en intercomparaciones, etc.

4.2 VIGENCIA DE LA AUTORIZACIÓN

19. La condición de laboratorio autorizado para la realización de MEMeC por parte del CCN, una vez concedida, se mantiene de manera indefinida, salvo renuncia expresa del laboratorio o incumplimiento de los requisitos REQ.1. o REQ.3.
20. En el caso de que el laboratorio se encuentre autorizado para un nivel de aseguramiento inferior al requerido para sucesivas evaluaciones, este deberá solicitar una nueva autorización para la ampliación del alcance al nivel de aseguramiento (CL) necesario y demostrar el cumplimiento de los REQ.2 y REQ.3 para dicho nivel de aseguramiento.
21. Adicionalmente, el CCN realizará una vigilancia continua de la competencia técnica del laboratorio autorizado en el transcurso de las actividades seguimiento de la evaluación MEMeC y durante la validación de los informes de evaluación emitidos por el laboratorio.
22. En el caso de observar un incumplimiento de los requisitos o un detrimento de la competencia técnica del laboratorio, el CCN notificará este hecho al laboratorio y establecerá un plazo y unas actividades a realizar para su subsanación.
23. El laboratorio deberá subsanar la causa que dio lugar a las observaciones o los incumplimientos en el plazo establecido.

24. La renuncia por parte del laboratorio, el incumplimiento REQ.1. o REQ.3., o la no subsanación de las observaciones recibidas, darán lugar a la **retirada total de la condición de laboratorio autorizado**.

4.3 LISTA DE LABORATORIOS AUTORIZADOS

25. El CCN mantendrá una relación actualizada de los laboratorios que se encuentran autorizados para la evaluación de productos conforme a la guía **CCN-STIC 2100 Metodología de Evaluación de Mecanismos Criptográficos (MEMeC) [REF3]**. Dicha relación se podrá consultar en la siguiente dirección electrónica: <https://oc.ccn.cni.es>.

5. REFERENCIAS

- REF1** Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.
- REF2** Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC).
- REF3** CCN-STIC 2100 *Cryptographic Mechanisms Evaluation Methodology* Metodología de Evaluación de Mecanismos Criptográficos (MEMeC).
- REF4** ORDEN PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.
- REF5** UNE-EN ISO/IEC 17025 Requisitos generales para la competencia de los laboratorios de ensayo y calibración.
- REF6** Real Decreto 1715/2010, de 17 de diciembre, por el que se designa a la Entidad Nacional de Acreditación (ENAC) como organismo nacional de acreditación de acuerdo con lo establecido en el Reglamento (CE) nº 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que deroga el Reglamento (CEE) nº 339/93.

6. ABREVIATURAS

CCN	Centro Criptológico Nacional
CL	Nivel de Certificación (<i>"Certification Level"</i>)
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
ENAC	Entidad Nacional de Acreditación
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
ISO/IEC	Organización Internacional de Normalización (<i>"International Organization for Standardization"</i>)/Comisión Electrotécnica Internacional (<i>"International Electrotechnical Commission"</i>)
MEMeC	Metodología de Evaluación de Mecanismos Criptográficos
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
UNE	Asociación Española de Normalización
VQ	Cuestionario del fabricante (<i>"Vendor Questionnaire"</i>)

