

ANCRA-PO-01

Procedimiento transitorio de notificación de Organismos de Evaluación de la Conformidad en el marco del CRA



24 de junio de 2026
Versión 1.0



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.

CONTROL DE VERSIONES

Versión	Fecha	Comentarios
0.1	20/04/2026	Versión inicial en formato borrador
0.2	04/06/2026	Implementación de cambios tras comentarios recibidos por parte de ENAC, de la Autoridad de Vigilancia del Mercado de CRA y de organismos interesados en ser notificados
0.3	12/06/2026	Implementación de cambios tras comentarios recibidos por parte de ENAC y de la Autoridad de Vigilancia del Mercado de CRA
1.0	24/06/2026	Versión inicial del documento para distribución pública

ÍNDICE

1. INTRODUCCIÓN	7
1.1 OBJETO	7
1.2 SITUACIÓN ACTUAL	7
2. ALCANCE.....	8
2.1 ALCANCE DEL DOCUMENTO EN EL CONTEXTO DE LA ACREDITACIÓN	9
3. MARCO JURÍDICO Y TÉCNICO	9
3.1 ELEMENTOS JURÍDICOS RELEVANTES DEL CRA.....	9
3.2 MARCO TÉCNICO APLICABLE EN AUSENCIA DE NORMAS ARMONIZADAS CRA	10
4. REQUISITOS DE LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD CRA. 12	
4.1 REQUISITOS TÉCNICOS	13
4.1.1 REQUISITOS TÉCNICOS SOBRE EL PRODUCTO	13
4.1.2 REQUISITOS TÉCNICOS SOBRE PROCESOS DEL FABRICANTE	13
4.1.3 COMPETENCIA TÉCNICA POR TIPO DE PRODUCTO.....	14
4.2 REQUISITOS FUNCIONALES	15
4.2.1 REQUISITOS PARA LA REVISIÓN DE LA DOCUMENTACIÓN TÉCNICA.....	15
4.2.2 REQUISITOS RELATIVOS A LOS MÓDULOS CRA.....	16
4.3 REQUISITOS HORIZONTALES	17
4.3.1 REQUISITOS ORGANIZATIVOS DEL OEC.....	17
4.3.2 REQUISITOS DE COMPETENCIA DEL PERSONAL DEL OEC	18
4.3.3 REQUISITOS PROCEDIMENTALES DE NOTIFICACIÓN	21
4.4 MATRIZ DE REQUISITOS Y RESPONSABILIDADES DEL OEC	22
5. REQUISITOS APLICABLES A LAS AUDITORÍAS DE AMPLIACIÓN DE ALCANCE CRA . 25	
5.1 REQUISITOS PARA ORGANISMOS DE CERTIFICACIÓN ACREDITADOS EN EL ESQUEMA EUCC	25
5.1.1 REQUISITOS ORGANIZATIVOS PARA ORGANISMOS EUCC.....	25
5.1.2 REQUISITOS DE COMPETENCIA DEL PERSONAL PARA ORGANISMOS EUCC	30
5.1.3 REQUISITOS TÉCNICOS Y FUNCIONALES PARA ORGANISMOS EUCC.....	32
5.1.4 REQUISITOS DE COMPETENCIA DEL OEC POR TIPO DE PRODUCTO	36
5.2 REQUISITOS PARA ORGANISMOS NOTIFICADOS CONFORME A LA DIRECTIVA 2014/53/UE (RED)	36
5.2.1 REQUISITOS ORGANIZATIVOS PARA ORGANISMOS RED	37
5.2.2 REQUISITOS DE COMPETENCIA DEL PERSONAL PARA ORGANISMOS RED.....	42
5.2.3 REQUISITOS TÉCNICOS Y FUNCIONALES PARA ORGANISMOS RED	45
5.2.4 REQUISITOS DE COMPETENCIA DEL OEC POR TIPO DE PRODUCTO	49
6. PROCEDIMIENTO DE LA AUTORIDAD NOTIFICANTE PARA LA NOTIFICACIÓN DE ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD CRA	50
6.1 ACTORES INVOLUCRADOS EN EL PROCEDIMIENTO Y SUS RESPONSABILIDADES .	50
6.2 REQUISITO PREVIO: ACREDITACIÓN PARA EL PROCEDIMIENTO TRANSITORIO PARA LA CRA MEDIANTE AUDITORÍA DE AMPLIACIÓN DE ALCANCE DE ENAC...	51
6.3 SOLICITUD DE NOTIFICACIÓN	52
6.4 TRAMITACIÓN DEL EXPEDIENTE POR LA AUTORIDAD NOTIFICANTE	53
6.5 RESULTADO DEL PROCEDIMIENTO	54
7. ACTUALIZACIÓN Y TRANSICIÓN FUTURA	54

ANEXOS	55
INTRODUCCIÓN	55
ANEXO A — MÓDULO A Y SU IMPACTO EN LA ACREDITACIÓN DEL OEC.....	56
A.1. OBJETO Y ALCANCE DEL ANEXO	56
A.2. NATURALEZA DEL MÓDULO A EN EL CRA	56
A.3. PAPEL DEL OEC RESPECTO AL MÓDULO A	57
A.4. CAPACIDADES ESPERABLES DEL OEC RELACIONADAS CON EL MÓDULO A	57
A.5. RELACIÓN CON OTROS MÓDULOS	57
ANEXO B — ORIENTACIONES PARA LA VERIFICACIÓN DE CAPACIDADES DEL OEC EN LA APLICACIÓN DEL MÓDULO B DEL CRA.....	58
B.1. OBJETO Y NATURALEZA DEL ANEXO	58
B.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA	58
B.3. NATURALEZA DEL MÓDULO B EN EL CRA.....	58
B.4. REPARTO DE RESPONSABILIDADES ENTRE CB E ITSEF	59
B.5. CAPACIDADES MÍNIMAS ESPERABLES DEL OEC PARA EL MÓDULO B.....	59
B.6. EVIDENCIAS TÍPICAS A VERIFICAR POR ENAC	59
B.7. RELACIÓN CON OTROS MÓDULOS Y CON LA DOCUMENTACIÓN CRA	59
ANEXO C — ORIENTACIONES SOBRE EL MÓDULO C Y SU INTEGRACIÓN EN LA ACTIVIDAD DEL OEC EN EL CRA.....	60
C.1. OBJETO Y NATURALEZA DEL ANEXO	60
C.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA	60
C.3. NATURALEZA DEL MÓDULO C EN EL CRA.....	60
C.4. PAPEL DEL OEC EN RELACIÓN CON EL MÓDULO C.....	61
C.5. INTEGRACIÓN DEL MÓDULO C EN LA EVALUACIÓN DE LA CONFORMIDAD	61
C.6. EVIDENCIAS ASOCIADAS A LA INTEGRACIÓN DEL MÓDULO C.....	61
C.7. RELACIÓN CON OTROS MÓDULOS	62
ANEXO H — ORIENTACIONES PARA LA VERIFICACIÓN DE CAPACIDADES DEL OEC EN LA APLICACIÓN DEL MÓDULO H	62
H.1. OBJETO Y NATURALEZA DEL ANEXO	62
H.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA	62
H.3. NATURALEZA DEL MÓDULO H EN EL CRA	63
H.4. RESPONSABILIDAD DEL ORGANISMO DE CERTIFICACIÓN (CB).....	63
H.5. PAPEL DE LAS ENTIDADES SUBCONTRATADAS	63
H.6. CAPACIDADES MÍNIMAS ESPERABLES DEL CB PARA EL MÓDULO H	64
H.7. EVIDENCIAS TÍPICAS A VERIFICAR POR ENAC	64
H.8. RELACIÓN CON OTROS MÓDULOS Y CON LA NOTIFICACIÓN CRA.....	64
REFERENCIAS.....	65
LEGISLACIÓN DE LA UNIÓN EUROPEA.....	65
NORMAS HORIZONTALES DE ACREDITACIÓN Y EVALUACIÓN DE LA CONFORMIDAD	65
NORMAS TÉCNICAS INCLUIDAS EN EL CONJUNTO DE REFERENCIAS TÉCNICAS VERIFICABLES (CRTV).....	65
DOCUMENTACIÓN EUROPEA SOBRE EL ESQUEMA EUCC Y LA ACREDITACIÓN DE ORGANISMOS.....	66
REFERENCIAS INTERNAS AL CRA.....	66

1. INTRODUCCIÓN

1.1 OBJETO

El objeto del presente documento es establecer un procedimiento transitorio para la evaluación de organismos de evaluación de la conformidad (CAB) interesados en convertirse en organismos notificados en el marco del Reglamento (UE) 2024/2847 (Cyber Resilience Act, CRA).

Se basa en la premisa de que, hasta la adopción de metodologías europeas específicas para la evaluación de la conformidad en el marco del CRA, únicamente los organismos que ya disponen de experiencia acreditada en esquemas consolidados de evaluación de la ciberseguridad, como EUCC o en el ámbito de la Directiva RED, están en condiciones de realizar evaluaciones CRA con garantías suficientes.

Por lo tanto, el procedimiento establece el mecanismo de notificación que se hará a través de auditorías de ampliación de alcance realizadas por ENAC, aplicadas a entidades que han demostrado capacidad técnica para evaluar requisitos de ciberseguridad establecidos en otros actos legislativos de la Unión Europea (EUCC o RED), y que, de acuerdo con las recomendaciones de la Comisión Europea, pueden acogerse a un mecanismo acelerado (*fast-track*).

Este procedimiento transitorio se aplicará mientras no existan criterios definitivos y armonizados a nivel de la Unión Europea para la evaluación de organismos a notificar y mientras los plazos habituales de acreditación puedan comprometer el cumplimiento del artículo 35.2 del Reglamento.

1.2 SITUACIÓN ACTUAL

El artículo 35.2 del Reglamento 2024/2847 (Cyber Resilience Act, CRA) exige que los Estados Miembros garanticen, antes del 11 de diciembre de 2026, un número suficiente de organismos notificados, de manera que se eviten cuellos de botella o retrasos en los procesos de evaluación de la conformidad. Para alcanzar este objetivo, los Estados Miembros deben designar sus autoridades notificantes y definir criterios de evaluación de los organismos candidatos a evaluar la conformidad de los productos con elementos digitales, preferiblemente mediante enfoques armonizados a nivel europeo. Sin embargo, los plazos habituales de los procesos de acreditación, aun siendo la vía preferente, pueden dificultar el cumplimiento del calendario previsto.

A esta dificultad estructural se suma que, en la fase actual de implantación del CRA, no existen aún los elementos normativos y técnicos necesarios para soportar los procesos de acreditación ni las funciones ordinarias de la Autoridad Notificante, dado que:

- no se han publicado normas armonizadas CRA en el Diario Oficial de la Unión Europea que permitan la presunción de conformidad prevista en el artículo 40 del CRA;

- la Comisión Europea no ha adoptado especificaciones comunes CRA conforme al artículo 27.2, que actúan como referencia obligatoria en ausencia de normas armonizadas;
- no se ha activado ningún esquema europeo de certificación como mecanismo de presunción de conformidad conforme al artículo 27.8 del CRA;
- los futuros estándares horizontales y verticales previstos para el CRA aún no han sido adoptados, por encontrarse en fases preliminares de elaboración por los organismos europeos de normalización.

En consecuencia:

- ENAC no dispone de una base técnica oficial sobre la que basar sus auditorías de ampliación de alcance para CRA;
- los organismos de evaluación de la conformidad no cuentan con normas CRA específicas para desarrollar sus procedimientos;
- la Autoridad Notificante carece de criterios comunes europeos que respalden designaciones o notificaciones.

Este vacío operativo afecta simultáneamente a ENAC, a los organismos evaluadores y a la Autoridad Notificante, generando la necesidad de adoptar medidas transitorias que sean técnicamente sólidas, trazables y jurídicamente aceptables.

Ante esta situación, y conforme a las indicaciones de la Comisión Europea, se considera adecuado habilitar un procedimiento acelerado (*fast-track*) para las entidades que ya han demostrado capacidad técnica para evaluar requisitos de ciberseguridad en otros actos legislativos de la Unión, permitiendo así avanzar en las evaluaciones previas a la notificación mientras se desarrollan los criterios armonizados y los mecanismos definitivos a nivel europeo. Para ello, se articula un **procedimiento transitorio basado en auditorías de ampliación de alcance realizadas por ENAC**, limitado exclusivamente a dichas entidades.

2. ALCANCE

Este procedimiento transitorio es aplicable a las entidades que, conforme a las recomendaciones de la Comisión Europea, pueden acogerse al mecanismo acelerado (*fast-track*) por haber demostrado capacidad técnica en la evaluación de requisitos de ciberseguridad en otros actos legislativos de la Unión, en particular:

- los organismos notificados conforme a la Directiva 2014/53/UE (RED) que estén acreditados conforme a ISO/IEC 17065, y cuya competencia técnica en ciberseguridad haya sido evaluada;
- los organismos de certificación acreditados conforme a ISO/IEC 17065 que operan en el esquema EUCC y desean ampliar su alcance para incluir actividades CRA.

Quedan excluidos de este mecanismo acelerado los laboratorios (ITSEF) acreditados bajo ISO/IEC 17025, que únicamente podrán participar mediante subcontratación o

convenio, conforme al artículo 41 del CRA, bajo la responsabilidad de un organismo de certificación.

Asimismo, este procedimiento es aplicable a:

- las actuaciones de la Autoridad Notificante relativas a la recepción, evaluación preliminar y preparación del expediente de notificación de las entidades comprendidas en el *fast-track*;
- las auditorías de ampliación de alcance realizadas por ENAC, que constituyen el mecanismo principal de evaluación durante este periodo.

2.1 ALCANCE DEL DOCUMENTO EN EL CONTEXTO DE LA ACREDITACIÓN

El presente documento incluye tanto requisitos evaluables en el marco de la acreditación como elementos de carácter procedimental o informativo.

A efectos de su aplicación por ENAC en auditorías de ampliación de alcance, únicamente serán objeto de verificación los requisitos del apartado 5.

Los demás apartados tendrán carácter informativo y no formarán parte del alcance de la auditoría de acreditación, sin perjuicio de su utilidad como referencia.

3. MARCO JURÍDICO Y TÉCNICO

El Reglamento (UE) 2024/2847 (CRA) constituye la base jurídica que define los requisitos esenciales de ciberseguridad, las obligaciones de los fabricantes y los criterios aplicables a los organismos de evaluación de la conformidad que deban ser designados y notificados. Dado el contexto transitorio descrito en el apartado 1.2 —en particular, la ausencia de normas armonizadas, especificaciones comunes CRA y estándares CRA adoptados— este apartado sintetiza el marco jurídico y técnico que sirve de fundamento para:

- estructurar el conjunto completo de requisitos CRA identificados en el apartado 4, y
- establecer el conjunto de requisitos adicionales que los certificadores tienen que cumplir para poder ser acreditados de acuerdo con el procedimiento transitorio descrito en este documento.

Este marco proporciona las referencias normativas y técnicas necesarias para que ENAC y la Autoridad Notificante puedan interpretar, de forma consistente y jurídicamente defendible, la aplicación del CRA durante el periodo transitorio.

3.1 ELEMENTOS JURÍDICOS RELEVANTES DEL CRA

El CRA establece un nuevo marco regulatorio europeo para la seguridad de productos con elementos digitales. Entre los elementos que afectan directamente a la actividad de los organismos de evaluación de la conformidad destacan:

- **Requisitos esenciales de ciberseguridad** (art. 6 y anexo I): establecen propiedades fundamentales de seguridad por diseño, seguridad por defecto, resistencia frente a ataques, gestión de vulnerabilidades y ciclo de vida seguro del producto.
- **Documentación técnica obligatoria** (art. 31 y anexo VII): define el contenido mínimo del expediente técnico que debe acompañar a cada producto evaluado.
- **Procedimientos y módulos de evaluación de la conformidad** (art. 32 y anexo VIII): especifican los módulos B, C y H y sus requisitos operativos, incluyendo examen UE de tipo, verificación de conformidad de producción y auditoría del sistema de calidad del fabricante.
- **Requisitos aplicables a los organismos notificados** (arts. 37 a 40): regulan la independencia, imparcialidad, competencia técnica y recursos de los organismos de evaluación de la conformidad (OEC).
- **Régimen de subcontratación** (art. 41): establece las condiciones bajo las cuales los OEC pueden apoyarse en laboratorios o entidades asociadas, manteniendo la responsabilidad última.
- **Procedimiento de designación y notificación** (arts. 42 a 45): determina cómo los organismos deben ser designados por la Autoridad Notificante e inscritos en el registro de la Comisión.

Estos elementos constituyen la referencia primaria sobre la que se han identificado y organizado los requisitos del apartado 4.

3.2 MARCO TÉCNICO APLICABLE EN AUSENCIA DE NORMAS ARMONIZADAS CRA

Ante la ausencia actual de normas armonizadas CRA y especificaciones comunes, ENAC utilizará un marco técnico formado por referencias consolidadas que permitan sustentar las auditorías de ampliación de alcance CRA durante el periodo transitorio. Este marco técnico está compuesto por los siguientes elementos:

a) Conjunto de Referencias Técnicas Verificables (CRTV)

El CRTV constituye el núcleo técnico común utilizado durante el periodo transitorio para evaluar los requisitos del CRA (Anexo I partes I y II, artículo 31 y módulos del artículo 32). El CRTV incluye las siguientes referencias técnicas:

- **ISO/IEC 15408** — Evaluación de la seguridad de productos de tecnologías de la información (Common Criteria).
- **ISO/IEC 18045** — Metodología de evaluación de la seguridad de productos de tecnologías de la información (Common Criteria Evaluation Methodology).
- **Perfiles de Protección (PP) de Common Criteria** (los del ámbito CCRA y EUCC, por ejemplo).
- Taxonomías y metodologías de evaluación del esquema nacional de certificación (LINCE, por ejemplo).
- **EN 17640** — Evaluación de **ciberseguridad** de productos TIC.

- **ETSI EN 303 645** — Requisitos de ciberseguridad para dispositivos IoT, cuando aplique.
- **ISO/IEC 29147** — Divulgación coordinada de vulnerabilidades.
- **ISO/IEC 30111** — Tratamiento de vulnerabilidades.
- **EN 18031** — Serie de normas de seguridad aplicables a equipos radioeléctricos.
- **IEC 62443** — Serie de normas relativas a la seguridad de sistemas industriales.

Las referencias incluidas en el CRTV no se aplican de forma uniforme en todos los casos, sino que su uso dependerá del tipo de producto, del contexto tecnológico y del alcance de la evaluación realizada.

Estas referencias podrán complementarse con borradores de estándares horizontales o verticales del CRA cuando ENAC y la Autoridad Notificante consideren que han alcanzado suficiente madurez para su aplicación.

b) Referencias técnicas complementarias

Además del CRTV, los organismos podrán utilizar, cuando resulte apropiado y esté técnicamente justificado, otras referencias técnicas adicionales.

Estas referencias pueden emplearse como métodos adicionales para reforzar el análisis de diseño, amenazas, vulnerabilidades y arquitectura, siempre que mantengan coherencia con los requisitos del CRA y con la trazabilidad método–resultado.

c) Experiencia técnica previa del organismo

Cuando sea pertinente, ENAC podrá considerar la experiencia previa del organismo en esquemas de evaluación existentes, siempre que dicha experiencia se encuentre alineada con el ámbito técnico del CRA.

d) Orientaciones sobre competencias del personal

ENAC tendrá en cuenta las orientaciones elaboradas por ENISA en materia de competencias del personal de organismos participantes en esquemas europeos de certificación de ciberseguridad (*Accreditation of CBs for EUCC, Accreditation of ITSEFs for EUCC* y *EUCC Guidelines Authorisation of CABs*), en la medida en que ayuden a interpretar el artículo 39.7 del CRA.

e) Normas horizontales de acreditación

El marco técnico se completa con las normas horizontales de acreditación cuya referencia ha sido publicada en el Diario Oficial de la Unión Europea, conforme a lo previsto en el artículo 40 del CRA. Estas normas —ISO/IEC 17065 para organismos de certificación de producto, proceso o servicio, ISO/IEC 17025 para laboratorios de ensayo— constituyen el marco aplicado por ENAC en las actividades de acreditación de este procedimiento transitorio.

Este conjunto técnico garantiza que las evaluaciones CRA realizadas durante el periodo transitorio se basan en referencias sólidas, coherentes y verificables, permitiendo a

ENAC fundamentar sus auditorías y proporcionando a la Autoridad Notificante un soporte adecuado para las decisiones de designación y notificación.

4. REQUISITOS DE LOS ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD CRA

El presente apartado recoge el marco general y completo de requisitos aplicables a cualquier Organismo de Evaluación de la Conformidad (OEC) que aspire a ser notificado en el ámbito del Reglamento (UE) 2024/2847 (CRA). Estos requisitos representan el nivel de cumplimiento integral que debe alcanzarse en condiciones normales de aplicación del CRA, con independencia del esquema previo de acreditación o notificación del que proceda la entidad (EUCC, RED u otros).

Este conjunto de requisitos constituyó el punto de partida para el análisis de brecha realizado por la Autoridad Notificante, al objeto de identificar las diferencias entre las capacidades de los organismos procedentes de esquemas existentes y las exigidas para operar como organismo notificado en el marco del CRA. En particular, permitió analizar de forma estructurada las capacidades ya disponibles en organismos EUCC o RED y determinar los requisitos adicionales necesarios para cumplir plenamente con el Reglamento.

Para estructurar de manera clara el marco general de requisitos CRA y alinearlos con la arquitectura del CRA y del Reglamento (UE) 765/2008, los requisitos se agrupan en tres bloques complementarios de carácter conceptual:

- **Requisitos técnicos**, relacionados con la capacidad del OEC para evaluar el cumplimiento de los requisitos esenciales del Anexo I, tanto sobre el producto como sobre los procesos del fabricante.
- **Requisitos funcionales**, vinculados a la revisión de la documentación técnica prevista en el artículo 31 y el Anexo VII y a la correcta operación de los módulos de evaluación de la conformidad establecidos en el artículo 32.
- **Requisitos horizontales**, que comprenden los elementos organizativos, de competencia del personal y los procedimientos internos necesarios para la acreditación, designación y notificación conforme al CRA y al Reglamento (UE) 765/2008.

La matriz del apartado 4.4 desarrolla cada uno de estos requisitos, su fundamento jurídico y su correspondencia con los marcos técnicos aplicables, proporcionando una visión estructurada y trazable del nivel de cumplimiento exigido a un OEC en el marco del CRA.

En el contexto del procedimiento transitorio descrito en este documento, **los requisitos que serán objeto de verificación durante el proceso acelerado (*fast-track*) son exclusivamente los definidos en el apartado 5**. Dicho apartado concreta el subconjunto de requisitos que se evaluarán en las auditorías de ampliación de alcance, permitiendo verificar de forma proporcionada la capacidad del organismo para operar conforme al CRA y poder ser notificado durante este periodo transitorio.

4.1 REQUISITOS TÉCNICOS

Este bloque recoge las capacidades técnicas necesarias para que el OEC pueda evaluar el cumplimiento de los requisitos esenciales establecidos en el Anexo I del CRA, según el tipo de producto, tanto respecto al diseño y comportamiento del producto como respecto a los procesos del fabricante.

4.1.1 REQUISITOS TÉCNICOS SOBRE EL PRODUCTO

Corresponden a la capacidad del OEC para evaluar los requisitos esenciales del Anexo I parte I del CRA, que incluyen la seguridad por diseño, la seguridad por defecto, la resistencia frente a ataques, la configuración segura y, cuando proceda, los aspectos relacionados con funciones criptográficas.

La evaluación técnica debe abarcar el análisis de la arquitectura del producto, sus superficies de ataque, los mecanismos de mitigación implementados y las evidencias de pruebas de seguridad aportadas por el fabricante. El OEC debe demostrar que dispone de metodologías, herramientas y procedimientos adecuados para identificar, analizar y verificar las medidas de seguridad del producto conforme a estos requisitos, manteniendo siempre la trazabilidad entre cada requisito evaluado, el método empleado y el resultado obtenido.

A efectos de este procedimiento transitorio, el OEC podrá emplear como base principal las referencias técnicas incluidas en el Conjunto de Referencias Técnicas Verificables (CRTV) recogidas en el apartado 3.2. Adicionalmente, podrá utilizar otros métodos cuando proceda, siempre que estén técnicamente justificados, sean coherentes con los requisitos del Anexo I, parte I, y se garantice la trazabilidad completa entre el requisito evaluado, el método aplicado, la evidencia obtenida y la conclusión alcanzada.

4.1.2 REQUISITOS TÉCNICOS SOBRE PROCESOS DEL FABRICANTE

Corresponden a la capacidad del OEC para evaluar los requisitos esenciales del Anexo I parte II del CRA, que regulan los procesos del fabricante asociados al ciclo de vida del producto, incluyendo el diseño, el desarrollo, la gestión de vulnerabilidades, la divulgación coordinada, el control de versiones, la gestión de dependencias y la aplicación de actualizaciones seguras durante todo el ciclo de vida.

La evaluación debe permitir confirmar que el fabricante dispone de procesos establecidos, documentados, implementados y efectivos para:

- gestionar vulnerabilidades conocidas y emergentes, incluyendo su identificación, clasificación, tratamiento y documentación;
- aplicar mecanismos adecuados para la divulgación coordinada de vulnerabilidades;
- mantener el control de versiones y de configuración del producto, incluidas las dependencias de software y hardware;
- gestionar actualizaciones de seguridad, parches y ciclos de mantenimiento;

- definir y aplicar un ciclo de vida seguro desde el diseño hasta el fin de vida del producto.

El OEC debe disponer de metodologías y herramientas que permitan evaluar estos procesos, revisar evidencias reales del fabricante y verificar que los procedimientos internos se ejecutan de forma sistemática y coherente con los requisitos del CRA. Asimismo, debe garantizar que existe trazabilidad entre cada requisito evaluado, la evidencia examinada y la conclusión alcanzada.

Durante el periodo transitorio, el OEC podría utilizar como referencias principales las normas incluidas en el Conjunto de Referencias Técnicas Verificables (CRTV) aplicables a procesos del fabricante, en particular ISO/IEC 29147 (divulgación de vulnerabilidades) y ISO/IEC 30111 (tratamiento y gestión de vulnerabilidades), así como, cuando proceda, secciones relevantes de EN 17640, ETSI EN 303 645, IEC 62443 o EN 18031.

Adicionalmente, podrán emplearse elementos específicos de las referencias del CRTV o metodologías técnicamente justificadas que refuercen la evaluación (por ejemplo, Perfiles de Protección (PP) o prácticas procedentes del esquema nacional LINCE), siempre que su aplicación esté técnicamente justificada y sea coherente con los objetivos del Anexo I parte II.

4.1.3 COMPETENCIA TÉCNICA POR TIPO DE PRODUCTO

Corresponde a la capacidad del OEC para integrar, de forma coherente y trazable, los requisitos técnicos del CRA aplicables a cada tipo de producto definido en los Anexos II y IV. Esta integración debe garantizar que la evaluación CRA combina adecuadamente:

- los requisitos esenciales de seguridad del producto (Anexo I parte I);
- los requisitos sobre los procesos del fabricante (Anexo I parte II);
- la revisión de la documentación técnica (artículo 31 y Anexo VII);
- y la aplicación de los módulos CRA (artículo 32 y Anexo VIII), cuando proceda.

El OEC debe demostrar que, para cada tipo de producto incluido en su alcance, dispone de un conjunto coherente de metodologías, herramientas y referencias técnicas que permiten cubrir todos los requisitos CRA aplicables. Durante el periodo transitorio, el OEC podrá emplear como referencia técnica principal el CRTV.

Esta integración debe reflejarse en:

- la identificación de las categorías de producto CRA (Anexos II y IV) que el organismo puede evaluar;
- una matriz interna que establezca la correspondencia estructurada entre cada tipo de producto, los requisitos CRA aplicables, los métodos técnicos utilizados en la evaluación, las competencias del personal asignado y las evidencias necesarias para demostrar su cumplimiento;
- procedimientos que aseguren el uso consistente del CRTV y de las referencias técnicas complementarias necesarias, manteniendo la correspondencia entre requisitos, métodos, evidencia y conclusión.

La integración de estos elementos debe permitir al OEC justificar, para cada tipo de producto, que la evaluación CRA es suficiente, consistente y trazable, y que se aplican métodos de evaluación acordes con el nivel de riesgo, la funcionalidad del producto y los requisitos del CRA.

4.2 REQUISITOS FUNCIONALES

Este bloque define las capacidades operativas necesarias para revisar y analizar la documentación técnica exigida por el CRA, así como para aplicar de forma efectiva los módulos de evaluación de la conformidad establecidos en el artículo 32.

4.2.1 REQUISITOS PARA LA REVISIÓN DE LA DOCUMENTACIÓN TÉCNICA

Corresponde a la capacidad del OEC para revisar la documentación técnica exigida por el artículo 31 y el Anexo VII del CRA, con el fin de verificar que el fabricante ha preparado un paquete de documentación técnica completo, coherente y suficiente para la evaluación de la conformidad. Esta revisión debe permitir confirmar que la documentación CRA describe de manera adecuada el diseño del producto, sus funcionalidades, los procesos aplicados por el fabricante y las medidas de seguridad implementadas durante todo su ciclo de vida.

La revisión documental debe abarcar, como mínimo, los siguientes elementos:

- arquitectura del producto y descripción detallada de sus componentes;
- diseño de seguridad, incluidas funcionalidades críticas, superficies de ataque y mecanismos de mitigación;
- análisis de riesgos y amenazas realizado por el fabricante;
- resultados de pruebas, ensayos y evaluaciones internas;
- información sobre dependencias, bibliotecas, componentes de terceros y cadena de suministro;
- documentación relativa al ciclo de vida seguro (actualizaciones, control de versiones, tratamiento de vulnerabilidades);
- manuales, instrucciones de uso y documentación de soporte destinada al usuario o integrador.

El OEC debe disponer de procedimientos y herramientas que aseguren que esta revisión se realiza de forma sistemática y trazable, permitiendo identificar carencias, incoherencias o evidencias insuficientes. Asimismo, debe demostrarse que existe trazabilidad entre los requisitos aplicables del CRA, los elementos revisados y las conclusiones emitidas por el organismo.

Durante el periodo transitorio, la revisión documental podrá apoyarse en las referencias técnicas incluidas en el Conjunto de Referencias Técnicas Verificables (CRTV), para contrastar la suficiencia de las evidencias aportadas por el fabricante.

El OEC deberá conservar íntegramente los expedientes CRA revisados, junto con todos los registros asociados a la revisión documental, garantizando su trazabilidad y

disponibilidad conforme a los requisitos de su sistema de gestión y a la normas de acreditación aplicable (ISO/IEC 17065). Esta conservación debe permitir a ENAC, durante la auditoría, y a la Autoridad Notificante, en cualquier momento, verificar la base técnica y documental sobre la que se emitieron las conclusiones de la evaluación.

4.2.2 REQUISITOS RELATIVOS A LOS MÓDULOS CRA

Corresponde a la capacidad del OEC para aplicar los módulos de evaluación de la conformidad establecidos en el artículo 32 y en el Anexo VIII del CRA. Cada módulo implica un conjunto específico de actividades y responsabilidades, que el organismo debe integrar en sus procedimientos internos, garantizando coherencia técnica, trazabilidad y cumplimiento de los requisitos CRA aplicables.

Aunque los módulos CRA relevantes para el ámbito del presente procedimiento son el B y el H, se incluyen también los módulos A y C, que aunque no implican intervención directa del organismo notificado en su aplicación aislada, sí definen los elementos esenciales (documentación técnica y control de producción) que son objeto de evaluación o referencia en otros módulos, especialmente el módulo B. Se pretende contribuir así a la coherencia e integridad del sistema de evaluación de la conformidad del CRA.

- **Módulo A — Control interno de la producción:**

El Módulo A es un módulo de autocontrol en el que no interviene ningún organismo notificado. El fabricante asume íntegramente la responsabilidad de la evaluación. El OEC no aplica este módulo, si bien, en el marco de otros módulos (especialmente el Módulo B), puede revisar la documentación técnica elaborada por el fabricante conforme al artículo 31 y al Anexo VII para verificar su completitud y coherencia.

- **Módulo B — Examen UE de tipo:**

El OEC debe realizar una evaluación técnica suficiente del tipo de producto, incluyendo análisis de diseño, arquitectura, superficies de ataque, evidencias de pruebas y mecanismos de mitigación. La evaluación debe determinar si el tipo cumple los requisitos esenciales del Anexo I parte I. Se debe mantener la trazabilidad entre requisitos evaluados, métodos técnicos aplicados y resultados obtenidos.

- **Módulo C — Conformidad con el tipo:**

En este módulo se verifica que la producción en serie mantiene la conformidad con el tipo evaluado en el Módulo B. Esto incluye la revisión de registros de fabricación, configuraciones, versiones de software/firmware, dependencias y evidencias de control de producción. La verificación debe asegurar que no existen desviaciones que afecten a la conformidad del producto con el CRA.

- **Módulo H — Garantía total de calidad:**

El OEC debe auditar el sistema de calidad del fabricante en relación con aspectos del ciclo de vida seguro, control de versiones, actualizaciones, dependencias y gestión de

vulnerabilidades. La evaluación debe confirmar que los procesos del fabricante cumplen lo dispuesto en el Anexo I parte II y que los mecanismos de control interno son eficaces, consistentes y verificables.

Durante el periodo transitorio, la aplicación de los módulos CRA podrá apoyarse en las referencias técnicas incluidas en el Conjunto de Referencias Técnicas Verificables (CRTV), cuando resulten pertinentes para los requisitos evaluados. Además, podrán emplearse el resto de elementos identificados en el apartado 3.2.

El OEC debe conservar la trazabilidad completa entre el módulo aplicado, los requisitos del CRA verificados, los métodos utilizados y las conclusiones emitidas. Asimismo, deberá mantener los registros, evidencias y expedientes generados en cada evaluación, conforme a su sistema de gestión y a las normas de acreditación aplicables.

4.3 REQUISITOS HORIZONTALES

Este bloque recoge los requisitos organizativos y de competencia del personal aplicables a los OEC, en consonancia con las normas horizontales de acreditación y con los artículos 39 a 41 del CRA.

4.3.1 REQUISITOS ORGANIZATIVOS DEL OEC

Los requisitos organizativos aplicables a los Organismos de Evaluación de la Conformidad (OEC) en el ámbito del CRA se basan en los artículos 39 a 41 del Reglamento y en las normas de acreditación ISO/IEC 17065.

Estos requisitos garantizan que el OEC opera con independencia, imparcialidad, competencia técnica, recursos adecuados, confidencialidad, y un sistema de gestión capaz de soportar actividades de evaluación de la conformidad de manera coherente con el marco legislativo del CRA.

El OEC debe demostrar que cumple los requisitos de los artículos 39 y 41 del Reglamento (UE) 2024/2847 y la norma ISO/IEC 17065.

Así mismo, el OEC debe demostrar que su sistema de gestión incorpora mecanismos específicos para actividades CRA, garantizando la imparcialidad en las decisiones técnicas, la adecuada separación funcional entre las actividades de evaluación y de decisión —asegurando que sean realizadas por personas distintas e independientes—, y la capacidad organizativa necesaria para integrar progresivamente los futuros estándares CRA una vez estén disponibles.

El OEC debe estar preparado para participar, cuando corresponda, en las actividades de coordinación de organismos notificados CRA organizadas por la Comisión o por la Autoridad Notificante, con el fin de favorecer la aplicación coherente del Reglamento y el intercambio de buenas prácticas.

4.3.2 REQUISITOS DE COMPETENCIA DEL PERSONAL DEL OEC

El artículo 39(7) del CRA exige que el personal responsable de llevar a cabo actividades de evaluación de la conformidad posea formación técnica adecuada, conocimientos suficientes de los requisitos evaluados, comprensión de los requisitos esenciales del anexo I y capacidad para elaborar certificados, registros e informes._

El OEC debe disponer de personal competente para desempeñar los roles necesarios en los módulos CRA para los que solicite acreditación, garantizando que el equipo evaluador cubre colectivamente todas las competencias técnicas, funcionales y organizativas asociadas y deberá tener en cuenta y las orientaciones técnicas elaboradas por ENISA para organismos notificados CRA.

Además, deberá disponer de mecanismos internos para asegurar el mantenimiento y la actualización continua de la competencia del personal asignado a actividades CRA, en coherencia con el alcance acreditado y con la evolución del marco normativo y técnico aplicable.

4.3.2.1 Funciones del personal del OEC

El organismo debe asignar funciones internas que permitan llevar a cabo de forma competente, independiente y trazable todas las actividades asociadas a la evaluación de la conformidad CRA, de acuerdo con su sistema de gestión y con la normas de acreditación aplicable (ISO/IEC 17065). Estas funciones no vienen definidas por el CRA, pero constituyen la estructura necesaria para demostrar el cumplimiento de los requisitos de competencia, imparcialidad y organización establecidos en el artículo 39 del CRA.

El organismo debe definir y asignar funciones diferenciadas para las actividades de revisión de la solicitud, evaluación, revisión y decisión de certificación, asegurando la competencia del personal, la independencia entre roles y la trazabilidad del proceso. Asimismo, debe garantizar la gestión del esquema, el control de la documentación y la preservación de la imparcialidad en todas las fases de la evaluación de la conformidad.

Estas funciones deben estar claramente descritas en el sistema de gestión del organismo y asignadas a personal competente.

4.3.2.2 Conocimientos y habilidades del personal evaluador

El personal evaluador debe poseer los conocimientos y habilidades necesarios para desempeñar de manera competente las actividades técnicas de evaluación CRA, en línea con los requisitos de competencia establecidos en el artículo 39 del CRA y con las obligaciones derivadas de las normas de acreditación horizontales. Estos conocimientos y habilidades tampoco vienen definidos explícitamente por el CRA, pero también constituyen la base técnica necesaria para evaluar los requisitos del anexo I, revisar la documentación técnica (artículo 31) y aplicar los módulos CRA que correspondan (artículo 32).

El personal evaluador debe demostrar:

a) Conocimientos generales

- Principios de ciberseguridad aplicables a productos con elementos digitales.
- Conceptos básicos de diseño y desarrollo seguro.
- Conocimientos sobre sistemas de gestión de calidad del fabricante cuando sean relevantes (módulo H).

b) Conocimientos de ciberseguridad del producto

- Ciclo de vida seguro, identificación de amenazas y superficie de ataque.
- Vulnerabilidades comunes, metodologías de análisis y su gestión.
- Principios de gestión criptográfica cuando sean pertinentes para la evaluación del tipo (módulo B).

c) Conocimientos de evaluación de la conformidad

- Terminología, principios y procesos del marco EN ISO/IEC 17000.
- Métodos de determinación, muestreo, revisión documental y análisis técnico utilizados en la evaluación CRA.

d) Habilidades técnicas

- Capacidades para realizar análisis técnicos, pruebas y ensayos cuando proceda.
- Capacidades de inspección técnica y análisis de evidencias.
- Habilidades de auditoría aplicables a procesos de fabricante cuando proceda (módulo H).

e) Habilidades generales

- Redacción clara y precisa de informes técnicos.
- Presentación de conclusiones técnicas ante revisores o decisores.
- Conducción de entrevistas técnicas con el fabricante.
- Dominio suficiente del idioma de trabajo de la evaluación.

f) Conocimiento y uso de referencias técnicas aplicables

El personal debe ser capaz de utilizar, cuando corresponda, las referencias técnicas incluidas en el CRTV y otros documentos técnicos pertinentes para el tipo de producto o familia tecnológica evaluada.

Cuando se empleen borradores de estándares horizontales o verticales del CRA, estos solo podrán utilizarse como referencias técnicas cuando posean el grado de madurez suficiente.

4.3.2.3 Competencias del jefe de evaluación

El jefe de evaluación debe demostrar:

- Visión transversal de todos los procesos de evaluación CRA.
- Capacidad de coordinar al equipo técnico.

- Validación de la idoneidad de los métodos aplicados.
- Habilidades avanzadas de comunicación técnica.
- Capacidad de justificar conclusiones ante el organismo de certificación.

4.3.2.4 Competencias del equipo de evaluación

El equipo evaluador debe cubrir colectivamente:

- Conocimientos completos sobre la familia de productos evaluada.
- Conocimiento del sector industrial del fabricante.
- Experiencia previa en análisis de vulnerabilidades, diseño seguro, ciclo de vida y actualizaciones.
- Conocimiento de las obligaciones y requisitos CRA aplicables.

4.3.2.5 Competencias del personal que prepara evaluaciones

Este personal debe poseer:

- Conocimientos de ciberseguridad y gestión de vulnerabilidades.
- Conocimiento de la terminología de evaluación de conformidad.
- Dominio de normas y esquemas aplicables (CRTV, CC, LINCE, RED...).
- Conocimiento suficiente del funcionamiento del OEC para estimar recursos.

4.3.2.6 Competencias del personal revisor y decisor

Debe cumplir:

- No haber estado involucrado en la evaluación.
- Conocimiento de principios de ciberseguridad y diseño seguro.
- Conocimientos sólidos de sistemas de calidad (especialmente módulo H).
- Conocimiento profundo de los procedimientos internos del OEC.
- Capacidad para juzgar la trazabilidad y suficiencia de la evidencia técnica.
- Dominio de los requisitos CRA, incluidos Anexo I, artículo 31 y artículos del módulo.

4.3.2.7 Experiencia, formación y cualificaciones

La competencia debe demostrarse mediante:

- Formación formal o certificaciones relevantes.
- Experiencia profesional en evaluación, auditoría, pruebas o gestión de vulnerabilidades.
- Participación en evaluaciones CRA, EUCC, CC, LINCE o RED.
- Formación continua y mantenimiento de competencias.

4.3.3 REQUISITOS PROCEDIMENTALES DE NOTIFICACIÓN

Los requisitos procedimentales asociados a la notificación de los Organismos de Evaluación de la Conformidad (OEC) en el ámbito del CRA derivan de los artículos 38, 42, 43, 44 y 45 del Reglamento, así como del Nuevo Marco Legislativo (NLF) y del Reglamento (CE) 765/2008. Estos requisitos garantizan la coherencia entre la acreditación otorgada por ENAC, la designación realizada por la Autoridad Notificante y el registro final del organismo notificado ante la Comisión Europea.

El OEC debe demostrar que dispone de procedimientos documentados, operativos y trazables para:

- **Solicitar la notificación inicial ante la Autoridad Notificante**, de acuerdo con los artículos 38 y 42 CRA, presentando un dossier completo que describa las actividades, módulos CRA y categorías de productos para los que solicita notificación.
- **Coherencia entre la notificación solicitada y el alcance acreditado por ENAC**, asegurando que el alcance técnico y organizativo está plenamente respaldado por evidencias verificadas durante la auditoría.
- **Gestión de subcontratación y entidades asociadas**, conforme al artículo 41 del CRA, incluyendo mecanismos de supervisión, responsabilidad última clara y control documental.
- **Comunicación de cambios relevantes**, en cumplimiento del artículo 45 del CRA, incluyendo cambios en estructura organizativa, personal clave, subcontratación, recursos o métodos de evaluación.
- **Actuar en caso de suspensión o retirada de su notificación**, cesando inmediatamente sus actividades en el alcance afectado, absteniéndose de emitir nuevos certificados y cooperando con la Autoridad Notificante mediante la información a las partes interesadas y la gestión o transferencia de los certificados y expedientes existentes, garantizando la continuidad y evitando riesgos en el mercado., en cumplimiento de las obligaciones derivadas del CRA y del marco del NLF.
- **Comunicación a la Autoridad Notificante de las certificaciones CRA emitidas, modificadas, suspendidas o retiradas**, cuando dicha información sea requerida por el CRA o por la normativa horizontal de vigilancia de mercado.
- **Interacción con la Autoridad Notificante**, garantizando que el organismo dispone de procedimientos documentados para interactuar con la Autoridad Notificante mediante procedimientos documentados que regulen la comunicación de información, la notificación de cambios y la respuesta a requerimientos.
- **Cooperación con las autoridades de vigilancia del mercado y otras autoridades competentes**, facilitando información sobre los expedientes CRA, las no conformidades graves detectadas y las medidas adoptadas, cuando así se le requiera.

Los procedimientos del OEC deben asegurar una interacción eficaz con la Autoridad Notificante, garantizar la coherencia documental de las solicitudes de notificación CRA y mantener trazabilidad completa entre la acreditación de ENAC, el alcance notificado y los módulos CRA aplicados. Asimismo, el OEC debe demostrar que estos procedimientos permiten una gestión controlada de cambios, suspensiones y retiradas conforme al artículo 45 del CRA, y que la información facilitada a la Autoridad Notificante es completa, precisa y compatible con el marco de supervisión del CRA.

4.4 MATRIZ DE REQUISITOS Y RESPONSABILIDADES DEL OEC

La matriz que se incluye en este apartado constituye el elemento central de trazabilidad del presente documento. En ella se recogen, de forma estructurada, los requisitos y responsabilidades aplicables a los Organismos de Evaluación de la Conformidad en el marco del CRA, organizados en áreas funcionales.

La matriz establece una correspondencia explícita entre:

- los requisitos generales definidos en el capítulo 4,
- las disposiciones jurídicas del CRA que les sirven de fundamento,
- y los requisitos específicos del apartado 5 aplicables a organismos procedentes de EUCC o del ámbito RED.

De este modo, la matriz 4.4 actúa como nexo operativo entre el marco general de requisitos CRA (capítulo 4), los criterios de evaluación del cumplimiento aplicados durante las auditorías de ampliación de alcance (capítulo 5) y las actividades de acreditación y notificación descritas en el capítulo 6.

La correspondencia entre los requisitos del capítulo 4 y su reflejo en la matriz no es estrictamente uno a uno, ya que algunos requisitos se desarrollan en varios ámbitos funcionales para facilitar su evaluación, mientras que otros se incorporan de forma directa en las filas correspondientes.

En conjunto, la matriz proporciona una visión integrada, coherente y trazable de las obligaciones que debe cumplir un organismo para operar conforme al CRA, permitiendo evaluar cada ámbito de forma clara, sistemática y defendible en el contexto de la acreditación.

Nota sobre las normas de acreditación y referencias técnicas

La verificación de los requisitos incluidos en la presente matriz se realiza en el marco de la acreditación conforme a ISO/IEC 17065, que constituye la referencia principal para la evaluación del cumplimiento de los requisitos organizativos, de competencia e imparcialidad del organismo de certificación.

Cuando las actividades de evaluación técnica se realicen mediante subcontratación, se tendrá en cuenta asimismo la norma ISO/IEC 17025 en relación con los requisitos aplicables a los laboratorios, de acuerdo con el artículo 41 del CRA.

Las demás referencias técnicas incluidas en el presente documento, en particular el Conjunto de Referencias Técnicas Verificables (CRTV) y otras referencias complementarias, tienen por objeto apoyar la verificación de las capacidades técnicas necesarias para la aplicación del CRA, sin constituir normas de acreditación en sentido estricto.

En caso de discrepancia entre los requisitos de ISO/IEC 17065 y otras referencias técnicas, prevalecerá lo establecido en ISO/IEC 17065 en tanto que base del proceso de acreditación.

#	Requisito CRA	Ref. CRA	Ref. Cap. 4	Ref. Cap. 5	Normas y Estándares de referencia	Responsabilidades del OEC
1	Organización, independencia, imparcialidad, sistema de gestión, recursos, confidencialidad, competencia	Art. 39	4.3.1	EUCC-ORG-1, EUCC-ORG-2, EUCC-ORG-3; RED-ORG-1, RED-ORG-2, RED-ORG-3	Normas horizontales (NO CRTV): ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17020, Reglamento (CE) 765/2008	Definir y aplicar un sistema de gestión que garantice independencia, imparcialidad, competencia técnica, confidencialidad y recursos adecuados para actividades CRA; participar, cuando proceda, en mecanismos de coordinación de organismos notificados. Para ello el OEC deberá demostrar que posee una acreditación en vigor según la norma ISO/IEC 17065 para el esquema EUCC o la directiva RED y que cumple los artículos 39 a 41 del CRA y lo demuestra mediante el cumplimiento de los criterios establecidos en este documento
2	Presunción de conformidad vía acreditación	Art. 40	3.2.e; 4.3.1	Base transversal del cap. 5	Normas horizontales (NO CRTV): ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17020, Reglamento (CE) 765/2008	Mantener la acreditación ENAC vigente y adecuada al alcance CRA
3	Subcontrataciones y filiales	Art. 41	4.3.1	EUCC-ORG-4; RED-ORG-4	Normas horizontales (NO CRTV): ISO/IEC 17025, ISO/IEC 17065, ISO/IEC 17020, Reglamento (CE) 765/2008	Definir y aplicar un modelo de subcontratación conforme al art. 41 CRA; seleccionar como subcontratistas a entidades competentes, evaluar y supervisar a las entidades subcontratadas; mantener la responsabilidad última sobre las actividades CRA subcontratadas
4	Capacidad para evaluar requisitos esenciales de seguridad del producto	Art. 6 + Anexo I parte I	4.1.1	EUCC-TEC-1; RED-TEC-1	CRTV: EN 17640; ETSI EN 303 645; ISO/IEC 29147; ISO/IEC 30111; IEC 62443; EN 18031 (cuando resulte aplicable en productos radioeléctricos o dispositivos conectados)	El OEC aplica metodologías de análisis de diseño, arquitectura, superficies de ataque y pruebas de seguridad; mapea requisitos CRA a métodos técnicos adecuados, utiliza referencias CRTV pertinentes y mantiene trazabilidad requisito-método-resultado. La revisión técnica verifica cobertura completa y trazabilidad
5	Capacidad para evaluar procesos del fabricante	Art. 6 + Anexo I parte II	4.1.2	EUCC-TEC-2; RED-TEC-2	CRTV: ISO/IEC 29147; ISO/IEC 30111; IEC 62443; EN	El OEC dispone de metodologías alineadas con las referencias técnicas del CRTV y de auditores competentes para evaluar los procesos del

					17640; ETSI EN 303 645; EN 18031 (cuando resulte aplicable a procesos asociados a dispositivos conectados o radioeléctricos)	fabricante (ciclo de vida, vulnerabilidades, dependencias, actualizaciones), así como de revisores competentes para verificar la cobertura y trazabilidad del proceso de auditoría, demostrando dicha competencia mediante evidencias de evaluaciones o auditorías realizadas en el ámbito EUCC, RED u otros contextos equivalentes
6	Revisión de la documentación técnica CRA	Art. 31 + Anexo VII	4.2.1	EUCC-TEC-3; RED-TEC-3	CRTV: EN 17640; ETSI EN 303 645; ISO/IEC 29147; ISO/IEC 30111; IEC 62443; EN 18031 (cuando resulte pertinente para validar la adecuación de la documentación técnica en productos radioeléctricos o entornos industriales)	El OEC dispone de procedimientos, listas de verificación y personal competente que revisa la documentación CRA del fabricante para comprobar que es completa y coherente, así como de personal revisor que verifique la completitud y coherencia de la revisión documental
7	Capacidad para aplicar el Módulo B (Examen UE de tipo)	Art. 32 + Anexo VIII (Módulo B)	4.2.2	EUCC-TEC-4; RED-TEC-4	CRTV: EN 17640; ETSI EN 303 645; ISO/IEC 29147; ISO/IEC 30111; IEC 62443	El personal evaluador técnico realiza la evaluación técnica del tipo aplicando correctamente el Módulo B, utilizando referencias técnicas pertinentes y garantizando la cobertura de los requisitos del Anexo I, manteniendo una trazabilidad completa entre requisitos, métodos, evidencias y resultados, con revisión independiente que verifique dicha cobertura
8	Capacidad para aplicar el Módulo H (Garantía total de calidad)	Art. 32 + Anexo VIII (Módulo H)	4.2.2	EUCC-TEC-4; RED-TEC-4	Procedimientos del fabricante; ISO/IEC 29147; ISO/IEC 30111; EN 17640 cuando aplique a procesos	El OEC cuenta con personal competente para auditar el sistema de calidad del fabricante y para realizar un proceso de revisión técnica que verifique coherencia y suficiencia de la evaluación.
9	Integración de requisitos CRA (producto, procesos y módulos)	Arts. 6, 31, 32 + Anexos I, VII, VIII	4.1.3	EUCC-PROD-1; RED-PROD-1	CRTV: EN 17640; ETSI EN 303 645; ISO/IEC 29147; ISO/IEC 30111; EN 18031 (cuando resulte aplicable)	El OEC cuenta con personal evaluador competente que integre evaluaciones de producto, procesos y módulos; y con personal revisor competente que verifique la coherencia global del proceso de evaluación
10	Procedimientos de notificación, comunicación y cooperación con autoridades	Arts. 38, 42-45	4.3.3	RED-ORG-5; base del cap. 6	SGC del organismo; procedimientos de notificación y comunicación	El OEC aplica procedimientos de comunicación de decisiones y cambios
11	Cooperación con autoridades y apoyo a la vigilancia del mercado	Arts. 38 y 55	4.3.3	RED-ORG-5 (vigilancia)	SGC del organismo; procedimientos de comunicación; mecanismos	El OEC coopera con autoridades y facilita información cuando se le requiera, disponiendo de procedimientos adecuados que garanticen dicha cooperación y la

					poscertificación	trazabilidad completa de las actuaciones realizadas
12	Gestión de cambios que afecten a la conformidad CRA	Arts. 43–45	4.3.3	RED-ORG-5 (gestión de cambios)	SGC del organismo; procedimientos de gestión de cambios; documentación CRA	El OEC gestiona cambios del producto y del fabricante, evaluando su impacto y comunicándolos cuando proceda

5. REQUISITOS APLICABLES A LAS AUDITORÍAS DE AMPLIACIÓN DE ALCANCE CRA

5.1 REQUISITOS PARA ORGANISMOS DE CERTIFICACIÓN ACREDITADOS EN EL ESQUEMA EUCC

La ampliación de alcance CRA en organismos de certificación previamente acreditados en el esquema EUCC exige verificar la adaptación de sus capacidades técnicas avanzadas al marco CRA. Dado que los organismos EUCC ya disponen de experiencia significativa en análisis técnico avanzado (Common Criteria/EUCC), revisión documental técnica, gestión de vulnerabilidades y evaluación de ciclo de vida, la brecha técnica entre EUCC y CRA es sustancialmente menor que en el caso de los organismos procedentes de RED.

Por este motivo, los requisitos incluidos en este apartado no pretenden establecer capacidades nuevas en sentido estricto, sino confirmar que las capacidades existentes en EUCC se han integrado adecuadamente en el enfoque CRA, especialmente en relación con los requisitos esenciales del Anexo I, la revisión documental del artículo 31 y la operación de los módulos B y H cuando correspondan. Se deberá verificar esta adaptación y su coherencia con el sistema de gestión del organismo.

5.1.1 REQUISITOS ORGANIZATIVOS PARA ORGANISMOS EUCC

5.1.1.1 Requisito EUCC-ORG-1 — Independencia e imparcialidad (externa e interna)

Definición del requisito

El OEC deben cumplir con los requisitos de imparcialidad e independencia establecidos en la norma ISO/IEC 17065 y en el artículo 39 del reglamento.

Explicación del requisito

Se asume que el Organismo de Certificación, al estar acreditado conforme a ISO/IEC 17065, dispone de mecanismos consolidados para garantizar la imparcialidad e independencia. En el contexto del CRA y, en particular, del artículo 39, el OC deberá asegurar que dichos principios se aplican específicamente a las actividades de evaluación de productos cubiertos por el Reglamento.

En particular, el OC deberá garantizar que:

- No participa, ni ha participado, en el diseño, desarrollo, fabricación, comercialización o mantenimiento de los productos evaluados bajo el CRA, ni presta servicios de consultoría asociados a los mismos.
- Las actividades de evaluación y la decisión de certificación son realizadas por personal distinto, garantizando una revisión independiente.
- Se identifican y gestionan posibles conflictos de interés derivados de relaciones con fabricantes, proveedores u otras partes implicadas en el ciclo de vida del producto.
- No existen influencias indebidas, en particular de carácter comercial o financiero, que puedan afectar a los resultados de las evaluaciones en el marco del CRA.

El OC deberá poder demostrar, cuando sea requerido, cómo sus mecanismos generales de imparcialidad (derivados de ISO/IEC 17065) han sido aplicados específicamente a las actividades cubiertas por el CRA.

Trazabilidad en este documento

- Apartado 4.3.1 (independencia, imparcialidad, separación entre evaluación y decisión).
- Matriz 4.4, fila 1.

Trazabilidad a normativa y estándares

- CRA: artículo 39 (requisitos aplicables a los organismos notificados) y artículo 40 (presunción de conformidad mediante acreditación).
- Normas horizontales: ISO/IEC 17065.
- Reglamento (CE) 765/2008 (requisitos generales de independencia e imparcialidad para organismos notificados en el marco del NLF).

5.1.1.2 Requisito EUCC-ORG-2 — Recursos humanos y técnicos adecuados para CRA

Definición del requisito

El Organismo de certificación debe disponer de recursos técnicos y humanos suficientes para las actividades de certificación CRA de su alcance.

Explicación del requisito

El organismo dispone de recursos humanos, técnicos y organizativos suficientes y proporcionados al alcance CRA solicitado, de modo que pueda desempeñar de forma efectiva y sostenida las actividades de evaluación de la conformidad correspondientes.

El CB debe asegurar que:

- El número, la cualificación y la disponibilidad del personal asignado a las actividades CRA son proporcionales al alcance solicitado y coherentes con las competencias técnicas exigidas por el Anexo I del CRA. A tal efecto, el organismo dispone de evaluadores, responsables de evaluación, revisores independientes

y personal decisor suficientes para cubrir los tipos de producto incluidos en el alcance, los módulos CRA solicitados (B y/o H) y el volumen de expedientes previsto.

- Tanto si el CB cuenta con medios internos, como si contrata ITSEFs pertenecientes a entidades diferenciadas para realizar las evaluaciones, se dispone de los medios técnicos, herramientas, equipamiento y metodologías necesarios para realizar análisis técnicos adecuados y utilizar técnicas pertinentes, como las indicadas en CRTV u otros métodos técnicamente justificados.
- El organismo de certificación (CB) demuestra una capacidad técnica real y efectiva, y no meramente administrativa, para participar en todas las fases de la evaluación CRA que requieren revisión independiente y adopción de decisiones de conformidad. Para el Módulo B, el CB dispone de recursos humanos y procedimientos propios para revisar de forma crítica los informes técnicos y adoptar decisiones de conformidad debidamente justificadas. Asimismo, el CB dispone de recursos humanos y organizativos suficientes para la correcta aplicación del Módulo H, incluyendo la auditoría y aprobación del sistema de calidad del fabricante y la evaluación de los procesos del ciclo de vida seguro, la gestión de vulnerabilidades, las actualizaciones y los controles internos. Estas funciones no pueden delegarse y se ejercen bajo la responsabilidad directa del CB.
- El organismo dispone, en conjunto, de recursos adecuados —humanos, materiales y organizativos— para integrar las actividades CRA en su operativa habitual, y su sistema de gestión permite asignar, mantener y demostrar la adecuación de dichos recursos de forma coherente con el alcance acreditado.

La acreditación ISO/IEC 17065 para el esquema EUCC o la directiva RED permite presumir el cumplimiento de determinados requisitos de imparcialidad y competencia. Así mismo la acreditación ISO/IEC 17025 para EUCC también permite presumir el cumplimiento de determinados requisitos de competencia técnica. Por lo tanto, no será necesario evaluar nuevamente esos requisitos en este procedimiento transitorio que se basará en la evaluación de los requisitos adicionales que no se demuestren mediante las acreditaciones mencionadas.

Trazabilidad en este documento

- Apartado 4.3.1 (recursos adecuados).
- Apartados 4.1 y 4.2 (capacidad técnica y funcional para evaluar requisitos CRA).

Trazabilidad normativa

- CRA: artículo 39 (capacidad técnica y disponibilidad de recursos)
- CRA: artículo 40 (presunción de conformidad mediante acreditación).
- Normas horizontales: ISO/IEC 17025 (laboratorios), ISO/IEC 17065 (organismos de certificación).

- CRTV: ISO/IEC 15408/18045, EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (cuando resulte aplicable).

5.1.1.3 Requisito EUCC-ORG-3 — Sistema de gestión documentado y operativo para CRA

Definición del requisito

El organismo debe disponer de un sistema de gestión (SG) documentado, implantado y operativo que incorpore procedimientos específicos para las actividades CRA y permita demostrar el cumplimiento de los requisitos técnicos, organizativos y procedimentales aplicables a los organismos notificados establecidos en el artículo 39 del CRA.

Explicación del requisito

El organismo debe disponer de un sistema de gestión documentado, implantado y operativo que integra de forma coherente las actividades CRA dentro de su organización.

El organismo debe contar con:

- procedimientos específicos para las actividades CRA, formalizados y bajo control del sistema de gestión, incluyendo la revisión de la documentación técnica conforme al artículo 31 del CRA, la aplicación de los módulos B, y/o H conforme al artículo 32 y al Anexo VIII, la gestión de la subcontratación conforme al artículo 41 y los procedimientos de notificación, gestión de cambios y comunicación con la Autoridad Notificante conforme a los artículos 42 a 45.
- un sistema de gestión que permita la gestión y conservación de los registros asociados a los expedientes CRA, incluyendo, cuando proceda, evaluaciones técnicas, revisiones independientes, decisiones de conformidad, control de imparcialidad, gestión de subcontratación y gestión de cambios.
- La documentación y los procedimientos CRA deben estar integrados de forma coherente con los procedimientos existentes del organismo, incluidos los derivados de esquemas previos como EUCC, evitando contradicciones, solapamientos o duplicidades en la operativa interna.
- una acreditación conforme a ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025, con un sistema de gestión implantado y un alcance adecuado a las actividades CRA, lo que permite presumir el cumplimiento de los requisitos organizativos, de competencia, imparcialidad y recursos establecidos en el artículo 39 del CRA, conforme a la presunción de conformidad prevista en su artículo 40.

El CRA exige que los organismos de evaluación de la conformidad dispongan de un sistema de gestión adecuado (artículo 39). A tal efecto, el artículo 40 del CRA reconoce la acreditación conforme a las normas horizontales de acreditación aplicables como el mecanismo para demostrar dicho cumplimiento, sin que sea necesario que ENAC verifique de nuevo de forma independiente cada uno de los requisitos del artículo 39 fuera del marco de la acreditación.

Trazabilidad en este documento

- 4.3.1 (existencia de SGC operativo).
- 4.2.1 y 4.2.2 (procedimientos CRA).
- Matriz 4.4, filas 1, 2, 3 y 4-9.

Trazabilidad normativa

- CRA: arts. 31, 32, 39, 41, 42–45.
- Normas horizontales: ISO/IEC 17025, 17065.
- Reglamento (CE) 765/2008 (requisitos generales para organismos notificados).

**5.1.1.4 Requisito EUCC-ORG-4 — Gestión de la subcontratación conforme al art. 41
CRA*****Definición del requisito***

El organismo debe aplicar un control formal, efectivo y trazable sobre toda actividad de subcontratación relacionada con la evaluación CRA, garantizando en todo caso que mantiene la responsabilidad final sobre las actividades subcontratadas, conforme al artículo 41 del CRA.

Explicación del requisito

Se debe comprobar que:

- Existen contratos o acuerdos formales con las entidades subcontratadas que describen claramente el alcance, responsabilidades y condiciones aplicables a actividades CRA.
- El organismo aplica criterios adecuados para la selección, evaluación y supervisión de subcontratación, compatibles con los requisitos CRA y con las normas horizontales de acreditación.
- Cada expediente CRA identifica de manera trazable qué actividades han sido subcontratadas y cómo el organismo ejerce el control y la responsabilidad final sobre dichas actividades.

Trazabilidad en este documento

- 4.3.1 (subcontratación).
- Matriz 4.4, fila 3 (Subcontrataciones y filiales).

Trazabilidad normativa

- CRA: art. 41.
- Normas horizontales: ISO/IEC 17025 / 17065 (control de subcontratación).

5.1.2 REQUISITOS DE COMPETENCIA DEL PERSONAL PARA ORGANISMOS EUCC

5.1.2.1 Requisito EUCC-COMP-1 — Cobertura de funciones necesarias para actividades CRA

Definición del requisito

El organismo debe disponer de personal competente que cubra todas las funciones necesarias para la evaluación de la conformidad CRA —tales como preparar evaluaciones, realizarlas, revisión y toma de decisión— de acuerdo con lo establecido en su sistema de gestión y en las normas de acreditación aplicables.

Explicación del requisito

El organismo deberá demostrar que:

- Dispone de una matriz de competencias que describe las funciones internas requeridas para realizar evaluaciones CRA.
- Cada función está cubierta por personal con formación y experiencia adecuadas, incluyendo cuando corresponda experiencia previa en EUCC/CC en actividades de análisis técnico, evaluación de vulnerabilidades, revisión documental y auditoría técnica. Estas actividades deben haber sido ejecutadas en el ámbito de, al menos, un expediente de evaluación cuyo informe técnico de evaluación haya obtenido un veredicto positivo por parte del organismo certificador.
- En los expedientes CRA, las funciones se asignan conforme a dicha matriz, garantizando la independencia e imparcialidad exigidas en el artículo 39 del CRA y en las normas de acreditación.
- La demostración de competencia del personal se apoya en evidencias tales como:
 - experiencia en métodos Common Criteria / ISO/IEC 15408 y 18045 (ADV, ATE, AVA, ALC), aplicables a la parte técnica de los requisitos del Anexo I CRA;
 - experiencia en revisiones de documentación técnica CRA conforme a lo dispuesto en el artículo 31 y el Anexo VII del CRA (ASE, AGD, etc.).
 - participación en evaluaciones basadas en EN 17640 (pruebas de penetración, pruebas funcionales, análisis de vulnerabilidades);
 - conocimientos de ETSI EN 303 645 (seguridad IoT) cuando sea pertinente al tipo de producto;
 - conocimientos de ISO/IEC 29147 y 30111 para la evaluación del proceso de gestión de vulnerabilidades del fabricante;
 - conocimientos de IEC 62443 (seguridad industrial) cuando sea pertinente al tipo de producto.

- El organismo es capaz de demostrar que el personal asignado a funciones de evaluación, revisión y decisión posee las competencias necesarias para aplicar las referencias técnicas correspondientes al alcance solicitado.

Trazabilidad en este documento - 4.3.2.1 (funciones del personal del OEC). - Matriz 4.4: filas 4–9

Trazabilidad normativa

- CRA: art. 39(7) (competencia del personal).
- Normas horizontales: ISO/IEC 17025 / 17065 (competencia, independencia y separación funcional).

5.1.2.2 Requisito EUCC-COMP-2 — Conocimiento y aplicación práctica del CRA y de las referencias técnicas aplicables

Definición del requisito

El personal debe conocer los requisitos del CRA aplicables a la evaluación de la conformidad (Anexo I, artículo 31 y módulos del artículo 32) y ser capaz de aplicarlos utilizando las referencias técnicas incluidas en el marco técnico aplicable definido en el apartado 3.2, cuando proceda para el tipo de producto o la actividad CRA correspondiente.

Explicación del requisito

El organismo debe demostrar que:

- El personal conoce los requisitos del CRA relevantes para la evaluación (Anexo I partes I y II, artículo 31 y los módulos del artículo 32), y puede explicarlos y aplicarlos correctamente en su ámbito de trabajo.
- El personal aplica de forma adecuada las referencias técnicas aplicables cuando resultan pertinentes para la evaluación CRA.
- El personal es capaz de explicar cómo se relacionan los requisitos del CRA con los métodos técnicos utilizados (ISO/IEC 17025 / 17065, ETSI EN 303 645, ISO/IEC 29147, 30111, IEC 62443, etc.), demostrando comprensión práctica de su aplicación en actividades reales o simuladas de evaluación CRA. Es decir:
 - Qué requisito CRA está evaluando.
 - Qué método del marco técnico aplicable (apartado 3.2) usa.
 - Por qué ese método es adecuado.
 - Qué evidencia genera.
 - Cómo esa evidencia demuestra cumplimiento.
- Dispone de evidencias en su Sistema de Gestión que ayuden a verificar este requisito (formación interna, participación en evaluaciones previas, revisiones documentales, análisis técnicos, expedientes representativos, etc).

Trazabilidad en este documento

- 4.3.2.2 (conocimientos y habilidades).
- Matriz 4.4: filas 4–9

Trazabilidad normativa

- CRA: arts. 6, 31, 32, Anexo I, Anexo VII.
- CRTV: ISO/IEC 15408/18045, EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (cuando resulte aplicable).

5.1.2.3 Requisito EUCC-COMP-3 — Experiencia práctica relevante equivalente a CRA***Definición del requisito***

El personal debe demostrar experiencia previa en actividades de evaluación equivalentes a las requeridas en CRA.

Explicación del requisito

El organismo deberá garantizar que:

- El personal CRA tiene participación documentada en evaluaciones EUCC, CC o LINCE.
- Dispone de experiencia en análisis de vulnerabilidades y ciclo de vida.
- La experiencia es verificable mediante expedientes en los que se ha participado como evaluador o supervisor.

Trazabilidad en este documento

- 4.3.2.7 (experiencia, formación y cualificaciones).
- Matriz 4.4: filas 4-9.

Trazabilidad normativa

- CRA: art. 39(7).
- Normas de referencia: ISO/IEC 15408, 18045.

5.1.3 REQUISITOS TÉCNICOS Y FUNCIONALES PARA ORGANISMOS EUCC**5.1.3.1 Requisito EUCC-TEC-1 — Evaluación de requisitos de ciberseguridad del producto*****Definición del requisito***

El organismo debe evaluar la conformidad del producto con los requisitos esenciales del Anexo I parte I del CRA, basándose en las metodologías técnicas que viene aplicando en el marco EUCC y utilizando, cuando dichas metodologías no cubran plenamente alguno de los requisitos, las metodologías definidas en el CRTV y complementarias, en función del tipo de producto evaluado.

Explicación del requisito

El organismo deberá demostrar que:

- Las metodologías técnicas utilizadas permiten evaluar de forma suficiente los atributos del Anexo I parte I del CRA (seguridad por diseño, seguridad por defecto, resistencia frente a ataques, configuración segura y gestión criptográfica cuando proceda), en función del tipo de producto evaluado y del nivel de aseguramiento aplicable.
- En caso de que una metodología concreta no cubra plenamente alguno de dichos atributos, el organismo ha definido y aplicado metodologías, extensiones o refinamientos técnicos adecuados, alineados con las referencias del CRTV.
- Las metodologías empleadas permiten documentar la trazabilidad entre cada requisito del Anexo I parte I, el método técnico utilizado para su evaluación y el resultado obtenido, de conformidad con los principios de evaluación del esquema EUCC.
- Utiliza referencias técnicas del CRTV y otras referencias técnicamente justificadas cuando proceda como marco técnico de referencia principal para la evaluación.

Trazabilidad en este documento

- 4.1.1 (requisitos técnicos del producto).
- Matriz 4.4, fila 4 (Capacidad para evaluar requisitos esenciales de seguridad del producto).

Trazabilidad normativa

- CRA: art. 6 y Anexo I parte I.
- CRTV: EN 17640, ISO/IEC 15408/18045, ETSI EN 303 645, IEC 62443.

5.1.3.2 Requisito EUCC-TEC-2 — Evaluación de procesos del fabricante definidos por el Anexo I parte II del CRA

Definición del requisito

El organismo acreditado conforme al esquema EUCC debe evaluar los procesos del fabricante relacionados con el ciclo de vida seguro del producto, la gestión de vulnerabilidades y la provisión de actualizaciones de seguridad, de acuerdo con los requisitos del Anexo I parte II del CRA, utilizando metodologías de evaluación y auditoría adecuadas al esquema EUCC, definiendo el nivel de aseguramiento aplicable y ajustando a dicho nivel el alcance, las evidencias y la profundidad de la evaluación.

Explicación del requisito

El organismo deberá demostrar que:

- Ha definido y aplica metodologías de evaluación específicas para EUCC que permitan evaluar los procesos del fabricante exigidos por el Anexo I parte II del CRA, diferenciando claramente entre:

- evaluación del producto, y
 - evaluación de procesos del fabricante.
- Evalúa de forma estructurada y sistemática los procesos del fabricante relativos, al menos, a:
 - gestión de vulnerabilidades (recepción, análisis, tratamiento y divulgación),
 - ciclo de vida seguro del producto,
 - provisión de actualizaciones de seguridad,
 - control de versiones y configuración,
 - gestión de dependencias relevantes para la seguridad.
- Utiliza referencias técnicas del CRTV (por ejemplo, ISO/IEC 29147 e ISO/IEC 30111) como marco técnico para la evaluación de dichos procesos, cuando resulten pertinentes para el tipo de producto y el nivel de aseguramiento evaluado.
- Solicita, revisa y evalúa evidencias reales del fabricante, tales como:
 - políticas y procedimientos documentados,
 - registros de gestión de vulnerabilidades,
 - historial de actualizaciones y parches de seguridad,
 - evidencias de control de configuración y versiones,
 - documentación del ciclo de vida seguro.
- Documenta la trazabilidad entre cada requisito aplicable del Anexo I parte II del CRA, el proceso del fabricante evaluado, la evidencia examinada y la conclusión alcanzada.

Trazabilidad en este documento

- 4.1.2 (procesos del fabricante).
- Matriz 4.4, fila 5 (Capacidad para evaluar procesos del fabricante).

Trazabilidad normativa

- CRA: art. 6 y Anexo I parte II.
- CRTV: ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (cuando resulten aplicables).

5.1.3.3 Requisito EUCC-TEC-3 — Revisión del expediente técnico CRA

Definición del requisito

El organismo debe poder revisar el expediente de evaluación CRA exigido por el artículo 31 y Anexo VII.

Explicación del requisito

El organismo deberá garantizar que:

- Revisa de manera sistemática la documentación técnica del producto (arquitectura, diseño, análisis de riesgos, resultados de pruebas, manuales y demás evidencias CRA exigidas por el Anexo VII).
- Se mantienen bajo control documental los registros asociados a las actividades CRA (incluyendo evaluación, decisiones, auditorías y subcontratación), conforme a los requisitos de gestión de registros establecidos en ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025.
- Dispone de listas de verificación o herramientas equivalentes específicas CRA, que permiten documentar la trazabilidad entre los requisitos aplicables y la documentación revisada.

Trazabilidad en este documento

- 4.2.1 (revisión documental).
- 4.3.1 (sistema de gestión de la calidad operativo).
- Matriz 4.4: filas 6-9.

Trazabilidad normativa

- CRA: art. 31, Anexo VII.

5.1.3.4 Requisito EUCC-TEC-4 — Operación correcta de los módulos CRA***Definición del requisito***

El organismo debe aplicar correctamente los módulos de evaluación de la conformidad del artículo 32 del CRA, conforme a lo previsto en el Anexo VIII.

Explicación del requisito

El organismo deberá garantizar que:

- En el **módulo B** (examen UE de tipo), aplica una evaluación técnica profunda utilizando referencias técnicas del CRTV cuando resulten pertinentes (por ejemplo, EN 17640, ISO/IEC 15408/18045, ETSI EN 303 645, IEC 62443).
- En el **módulo H** (sistema de calidad), evalúa el sistema de calidad del fabricante, incluyendo el ciclo de vida seguro, la gestión de vulnerabilidades, las actualizaciones y los procesos de control interno.

Trazabilidad en este documento

- 4.2.2 (módulos CRA).
- Matriz 4.4, filas 7 y 8.

Trazabilidad normativa

- CRA: art. 32 y Anexo VIII.

5.1.4 REQUISITOS DE COMPETENCIA DEL OEC POR TIPO DE PRODUCTO

5.1.4.1 Requisito EUCC-PROD-1 — Competencia técnica por tipo de producto (Anexos II y IV CRA)

Definición del requisito

El organismo debe demostrar competencia técnica específica para cada tipo de producto CRA incluido en su solicitud de alcance, de acuerdo con los requisitos del Anexo I del CRA y con las familias de productos definidas en los Anexos II y IV.

Explicación del requisito

El organismo deberá demostrar que:

- Que el organismo identifica explícitamente las familias o tipos de producto CRA incluidos en su solicitud de notificación, de acuerdo con los Anexos II y IV del CRA.
- Que existe una correspondencia clara y justificada entre las capacidades técnicas previas del organismo (por ejemplo, experiencia en esquemas EUCC/Common Criteria) y los tipos de producto para los que se solicita la notificación conforme al CRA.
- Que el organismo dispone de una matriz documentada en la que, para cada tipo de producto CRA solicitado, se identifican los métodos técnicos del CRTV aplicables y las competencias del personal asignado a su evaluación, garantizando que cada tipo de producto cuenta con los recursos técnicos y humanos necesarios.
- Que el organismo dispone de herramientas, equipamiento y plataformas de prueba adecuadas y coherentes con las características técnicas de cada tipo de producto CRA evaluado.

Trazabilidad en este documento

- 4.1.1, 4.1.2, 4.2.1, 4.3.2.
- Matriz 4.4, filas 4, 5 y 11.

Trazabilidad normativa

- CRA: art. 6, Anexos I, II, IV.
- CRTV: ISO/IEC 15408/18045, EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (cuando resulte aplicable).

5.2 REQUISITOS PARA ORGANISMOS NOTIFICADOS CONFORME A LA DIRECTIVA 2014/53/UE (RED)

La ampliación de alcance al CRA en organismos notificados conforme a la Directiva 2014/53/UE (RED) requiere una verificación más amplia que en el caso de organismos procedentes de otros esquemas como el EUCC, ya que, si bien el ámbito RED incluye la

evaluación de la conformidad mediante la revisión del expediente técnico del fabricante —incluyendo ensayos, análisis de diseño, revisión documental y verificación del cumplimiento en base a normas armonizadas o especificaciones técnicas—, no cubre de forma completa ni sistemática todos los elementos que el CRA exige evaluar.

En particular, el CRA introduce obligaciones adicionales o más exigentes en aspectos como la gestión de vulnerabilidades, el ciclo de vida seguro, las actualizaciones de seguridad y la integración estructurada de estos elementos en la evaluación de la conformidad, así como una mayor exigencia de trazabilidad entre requisitos, métodos, evidencias y conclusiones.

En consecuencia, la brecha técnica y procedimental entre RED y CRA es mayor que en el caso de organismos con experiencia en esquemas específicamente orientados a la ciberseguridad, no tanto por la naturaleza de las actividades realizadas, sino por el nivel de profundidad, sistematización y alcance requerido. El paso desde RED hacia CRA implica, por tanto, reforzar y estructurar capacidades técnicas existentes, incluyendo el análisis detallado del diseño del producto, la auditoría de los procesos del fabricante y la aplicación de los módulos del artículo 32 del CRA con un mayor nivel de rigor metodológico y trazabilidad.

Por ello, los requisitos incluidos en este apartado se centran en verificar, mediante evidencia práctica, que el organismo notificado RED ha adquirido y formalizado las capacidades necesarias para operar conforme al CRA, tanto en su vertiente técnica (evaluación completa de los requisitos del Anexo I, revisión documental y auditoría de procesos del fabricante) como en su vertiente procedimental (sistema de gestión, imparcialidad, trazabilidad y aplicación de los módulos B y H). Esta verificación permite confirmar que el organismo está en condiciones de desempeñar adecuadamente las actividades conforme al procedimiento transitorio en el marco del CRA con la profundidad, el alcance y la fiabilidad requeridos por el Reglamento.

5.2.1 REQUISITOS ORGANIZATIVOS PARA ORGANISMOS RED

5.2.1.1 Requisito RED-ORG-1 — Independencia e imparcialidad aplicadas al contexto CRA

Definición del requisito

El organismo debe demostrar independencia e imparcialidad en todas las actividades CRA, garantizando la ausencia de interferencias entre actividades de ensayo, evaluación técnica, revisión y decisión.

Explicación del requisito

El organismo cumple los requisitos de independencia e imparcialidad establecidos en el artículo 39 del CRA, conforme a su acreditación y al sistema de gestión aplicable.

A tal efecto, deberá verificarse que el organismo dispone de una estructura organizativa, políticas de imparcialidad y mecanismos de control que garantizan la separación entre

las actividades de evaluación técnica y la adopción de decisiones de conformidad, en coherencia con las prácticas exigidas por ISO/IEC 17065.

La acreditación ISO/IEC 17065 para el esquema EUCC o la directiva RED permite presumir el cumplimiento de determinados requisitos de imparcialidad e independencia. Así mismo la acreditación ISO/IEC 17025 para EUCC también permite presumir el cumplimiento de determinados requisitos de imparcialidad. Por lo tanto, no será necesario evaluar nuevamente esos requisitos en este procedimiento transitorio que se basará en la evaluación de los requisitos adicionales que no se demuestren mediante las acreditaciones mencionadas.

Trazabilidad en este documento

- 4.3.1 (independencia, imparcialidad).
- Matriz 4.4, fila 1.

Trazabilidad normativa

- CRA: art. 39.
- ISO/IEC 17025, ISO/IEC 17065.
- Reglamento (CE) 765/2008.

5.2.1.2 Requisito RED-ORG-2 — Suficiencia de recursos para actividades CRA

Definición del requisito

El organismo debe disponer de recursos humanos, técnicos y procedimentales adecuados para realizar evaluaciones CRA, más allá de los recursos propios del esquema RED.

Explicación del requisito

El organismo dispone de recursos humanos, técnicos y organizativos suficientes y proporcionados al alcance CRA solicitado, de modo que pueda desempeñar de forma efectiva y sostenida las actividades de evaluación de la conformidad correspondientes.

En particular, el organismo deberá garantizar que:

- El número, la cualificación y la disponibilidad del personal asignado a las actividades CRA son proporcionales al alcance solicitado y coherentes con las competencias técnicas exigidas por el Anexo I del CRA. A tal efecto, el organismo dispone de evaluadores, responsables de evaluación, revisores independientes y personal decisor suficientes para cubrir los tipos de producto incluidos en el alcance, los módulos CRA solicitados (B y/o H), el volumen de expedientes previsto y las exigencias de separación funcional derivadas de la acreditación conforme a ISO/IEC 17065.
- Dispone de los medios técnicos, herramientas, infraestructuras y metodologías necesarias para realizar las actividades técnicas asociadas al Módulo B, ya sea mediante recursos propios o mediante subcontratación conforme al artículo 41

del CRA y a las normas de acreditación aplicables, utilizando referencias técnicas pertinentes y métodos técnicamente justificados.

- Demuestra una capacidad técnica real y efectiva, y no meramente administrativa, para participar en todas las fases de la evaluación CRA que requieren revisión independiente y adopción de decisiones de conformidad. En el Módulo B, el organismo dispone de recursos humanos y procedimientos propios para revisar de forma crítica los resultados de la evaluación técnica y adoptar decisiones de conformidad debidamente justificadas. Asimismo, dispone de recursos humanos y organizativos suficientes para la correcta aplicación del Módulo H, incluyendo la auditoría y aprobación del sistema de calidad del fabricante y la evaluación de los procesos del ciclo de vida seguro, la gestión de vulnerabilidades, las actualizaciones y los controles internos. Estas funciones no pueden delegarse y se ejercen bajo la responsabilidad directa del organismo.
- Dispone, en conjunto, de recursos adecuados —humanos, materiales y organizativos— para integrar las actividades CRA en su operativa habitual, y su sistema de gestión permite asignar, mantener y demostrar la adecuación de dichos recursos de forma coherente con el alcance acreditado.

La acreditación ISO/IEC 17065 para el esquema EUCC o la directiva RED permite presumir el cumplimiento de determinados requisitos organizativos, de competencia, imparcialidad y recursos. Así mismo la acreditación ISO/IEC 17025 para EUCC también permite presumir el cumplimiento de determinados requisitos. Por lo tanto, no será necesario evaluar nuevamente esos requisitos en este procedimiento transitorio que se basará en la evaluación de los requisitos adicionales que no se demuestren mediante las acreditaciones mencionadas.

Trazabilidad en este documento

- 4.3.1 (recursos adecuados).
- 4.1 y 4.2 (requisitos técnicos y funcionales).
- Matriz 4.4, filas 1–10.

Trazabilidad normativa

- CRA: art. 39.
- Referencias técnicas del CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443.

5.2.1.3 Requisito RED-ORG-3 — Sistema de gestión adaptado a CRA

Definición del requisito

El organismo debe disponer de un sistema de gestión documentado y operativo que incorpore procedimientos específicos para las actividades CRA, complementarios a los procedimientos RED existentes.

Explicación del requisito

El organismo deberá demostrar que: dispone de un sistema de gestión documentado, implantado y operativo que integra de forma coherente las actividades CRA dentro de su organización.

En particular, el organismo deberá garantizar que:

- Existen procedimientos específicos para las actividades CRA, formalizados y bajo control del sistema de gestión, incluyendo la revisión de la documentación técnica conforme al artículo 31 del CRA, la aplicación de los módulos B y/o H conforme al artículo 32 y al Anexo VIII, la gestión de la subcontratación conforme al artículo 41 y los procedimientos de notificación, gestión de cambios y comunicación con la Autoridad Notificante conforme a los artículos 42 a 45.
- El sistema de gestión permite la gestión y conservación de los registros asociados a los expedientes CRA, incluyendo evaluaciones técnicas, revisiones independientes, decisiones de conformidad, control de imparcialidad, gestión de subcontratación y gestión de cambios.
- La documentación y los procedimientos CRA están integrados de forma coherente con los procedimientos existentes del organismo, evitando contradicciones, solapamientos o duplicidades en la operativa interna.
- Dispone de una acreditación conforme a ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025, con un sistema de gestión implantado y un alcance adecuado a las actividades CRA, lo que permite presumir el cumplimiento de los requisitos organizativos, de competencia, imparcialidad y recursos establecidos en el artículo 39 del CRA, conforme a la presunción de conformidad prevista en su artículo 40.

El CRA exige que los organismos de evaluación de la conformidad dispongan de un sistema de gestión adecuado (artículo 39). A tal efecto, el artículo 40 del CRA reconoce la acreditación conforme a las normas horizontales de acreditación aplicables como el mecanismo para demostrar dicho cumplimiento, sin que sea necesario que ENAC verifique de nuevo de forma independiente cada uno de los requisitos del artículo 39 fuera del marco de la acreditación.

Trazabilidad en este documento

- 4.3.1 (sistema de gestión).
- Matriz 4.4, fila 1 y filas 6–10.

Trazabilidad normativa

- CRA: arts. 31, 32, 39, 42–45.
- ISO/IEC 17025 ISO/IEC 17065.

5.2.1.4 Requisito RED-ORG-4 — Gestión de la subcontratación conforme al CRA

Definición del requisito

El organismo debe aplicar un control formal, efectivo y trazable sobre todas las actividades de subcontratación vinculadas a la evaluación CRA, manteniendo la responsabilidad final conforme al artículo 41 CRA.

Explicación del requisito

El organismo deberá garantizar que:

- No se externalizan actividades esenciales de evaluación CRA sin un control adecuado.
- Existen procedimientos CRA para seleccionar, supervisar y evaluar entidades subcontratadas.
- Las actividades críticas vinculadas a la evaluación del anexo I o a la operación de los módulos CRA se supervisan de forma efectiva.

Trazabilidad en este documento

- 4.3.1 (subcontratación).
- Matriz 4.4, fila 3.

Trazabilidad normativa

- CRA: art. 41.
- ISO/IEC 17025, ISO/IEC 17065.

5.2.1.5 Requisito RED-ORG-5 — Procedimientos de notificación y cooperación con autoridades

Definición del requisito

El organismo debe disponer de procedimientos CRA que permitan la comunicación estructurada y la cooperación con la Autoridad Notificante y con las autoridades de vigilancia del mercado.

Explicación del requisito

El organismo deberá garantizar que:

- Puede comunicar certificados CRA emitidos, modificados, suspendidos o retirados.
- Dispone de procedimientos para responder a requerimientos de autoridades de vigilancia del mercado.
- El sistema de gestión garantiza la trazabilidad de las decisiones de conformidad CRA, de manera que cada decisión adoptada esté documentada, justificada y vinculada a las evidencias técnicas, revisiones y actuaciones realizadas.

Trazabilidad en este documento

- 4.3.3 (requisitos procedimentales).
- Matriz 4.4, fila 12.

Trazabilidad normativa

- CRA: arts. **38, 42–45**.
- Reglamento (CE) **765/2008**.

5.2.2 REQUISITOS DE COMPETENCIA DEL PERSONAL PARA ORGANISMOS RED**5.2.2.1 Requisito RED-COMP-1 — Conocimiento detallado del CRA y del CRTV*****Definición del requisito***

El personal debe comprender los requisitos CRA aplicables (anexo I, artículo 31 y módulos del artículo 32) y ser capaz de aplicarlos utilizando las referencias técnicas pertinentes incluidas en el CRTV.

Explicación del requisito

El organismo deberá garantizar que:

- El personal domina los requisitos del CRA aplicables (Anexo I partes I y II, artículo 31 y módulos CRA).
- El personal conoce y aplica referencias técnicas del CRTV cuando resultan pertinentes.
- La formación y competencia CRA está documentada y evaluada internamente.

La competencia del personal deberá estar respaldada por evidencias objetivas. A tal efecto, se podrá comprobar, entre otros, los siguientes elementos:

- Formación específica en requisitos CRA y ciberseguridad de producto.
- Experiencia previa en evaluación de seguridad o certificación (por ejemplo, en el ámbito RED, Common Criteria u otras metodologías equivalentes).
- Participación en actividades de evaluación técnica o revisión documental.
- Registros de cualificación interna y evaluación de competencias del personal.

Trazabilidad en este documento

- 4.3.2.2 (competencias).
- Matriz 4.4, filas 4–11.

Trazabilidad normativa

- CRA: arts. 6, 31, 32, 39(7).
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, ISO/IEC 15408/18045, IEC 62443 y EN 18031 (cuando resulten aplicables)

5.2.2.2 Requisito RED-COMP-2 — Competencias en análisis de diseño y arquitectura***Definición del requisito***

El personal debe ser capaz de evaluar el diseño del producto, su arquitectura, superficies de ataque y mecanismos de mitigación.

Explicación del requisito

El organismo deberá garantizar que:

- El organismo es capaz de evaluar el diseño del producto, su arquitectura y la adecuación del expediente técnico del fabricante, incluyendo la revisión de la documentación técnica, las especificaciones de diseño y los procesos de fabricación, y dispone de personal con los conocimientos y experiencia necesarios para realizar dicho análisis, incluyendo la identificación de superficies de ataque y la valoración de las medidas de seguridad implementadas para su mitigación cuando resulte aplicable.

La competencia del personal deberá estar respaldada por evidencias objetivas. A tal efecto, se podrá comprobar, entre otros, los siguientes elementos:

- Desarrollo o revisión de análisis de arquitectura de producto, incluyendo:
 - identificación de componentes, interfaces y flujos de datos, - análisis de superficies de ataque (interfaces expuestas, comunicaciones, dependencias externas).
- Evaluaciones en las que se hayan identificado o analizado:
 - amenazas y vectores de ataque relevantes, - mecanismos de mitigación (autenticación, control de acceso, actualización segura, etc.).
- Evaluaciones en las que se haya realizado revisión técnica del expediente del fabricante, incluyendo documentación de diseño, arquitectura y especificaciones del producto.
- Uso documentado de métodos o marcos de análisis técnico en expedientes de evaluación de la ciberseguridad, tales como:
 - modelado de amenazas, - análisis de arquitectura, - revisión estructurada de requisitos de seguridad.
- Experiencia previa en evaluación de seguridad de producto (por ejemplo, en entornos RED que incluyan requisitos de ciberseguridad, Common Criteria u otros esquemas equivalentes).
- Registros internos que acrediten la cualificación del personal y su asignación a actividades de análisis técnico.

Trazabilidad en este documento

- 4.1.1 (requisitos del producto).
- Matriz 4.4, fila 4.

Trazabilidad normativa

- CRA: Anexo I parte I.

- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, ISO/IEC 15408/18045, IEC 62443.

5.2.2.3 Requisito RED-COMP-3 — Competencias en ciclo de vida seguro y gestión de vulnerabilidades

Definición del requisito

El personal debe demostrar competencia en la auditoría de procesos de ciclo de vida seguro y gestión de vulnerabilidades.

Explicación del requisito

El organismo deberá garantizar que:

- El personal conoce las referencias técnicas del CRTV aplicables a la gestión de vulnerabilidades y ciclo de vida seguro (ISO/IEC 29147 y ISO/IEC 30111).
- El personal dispone de conocimientos y experiencia para auditar procesos del fabricante relacionados con:
 - divulgación coordinada de vulnerabilidades,
 - gestión de dependencias y componentes,
 - control de cambios y actualizaciones,
 - mantenimiento de la seguridad a lo largo del ciclo de vida del producto.
- El personal es capaz de evaluar los requisitos del Anexo I parte II del CRA en el contexto de procesos organizativos del fabricante.

La competencia del personal deberá estar respaldada por evidencias objetivas. A tal efecto, se podrá comprobar, entre otros, los siguientes elementos:

- Participación en auditorías o evaluaciones de procesos relacionados con gestión de vulnerabilidades o ciclo de vida seguro.
- Revisión documentada de procedimientos de fabricante tales como:
 - gestión de vulnerabilidades,
 - políticas de divulgación,
 - gestión de parches y actualizaciones,
 - control de versiones y cambios.
- Uso de metodologías o enfoques estructurados para evaluar procesos (por ejemplo, revisión de procesos, análisis de evidencias documentales o auditoría de procedimientos).
- Formación o experiencia en gestión de vulnerabilidades y ciclo de vida de desarrollo seguro.
- Registros internos de cualificación y asignación del personal a actividades de auditoría de procesos.

Trazabilidad en este documento

- 4.1.2.

- Matriz 4.4, fila 5.

Trazabilidad normativa

- CRA: Anexo I parte II.
- CRTV: ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (estas dos últimas, cuando resulten aplicables).

5.2.2.4 Requisito RED-COMP-4 — Competencias en revisión de documentación técnica CRA

Definición del requisito

El personal debe poder revisar la documentación técnica CRA, incluyendo análisis de riesgos, arquitectura, diseño, pruebas y documentación del fabricante.

Explicación del requisito

El organismo deberá garantizar que:

- Utiliza plantillas de revisión documental CRA alineadas con el artículo 31 y el anexo VII.
- El personal sabe evaluar la coherencia entre documentación técnica y requisitos del CRA.
- La revisión CRA no se limita a documentación o ensayos RED.

Trazabilidad en este documento

- 4.2.1.
- Matriz 4.4, fila 6.

Trazabilidad normativa

- CRA: art. 31, Anexo VII.
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (estas dos últimas, cuando resulten aplicables).

5.2.3 REQUISITOS TÉCNICOS Y FUNCIONALES PARA ORGANISMOS RED

5.2.3.1 Requisito RED-TEC-1 — Evaluación de requisitos de ciberseguridad del producto

Definición del requisito

El organismo debe evaluar la conformidad del producto con los requisitos esenciales del Anexo I parte I del CRA, basándose en las metodologías técnicas que viene aplicando en el marco RED y utilizando, cuando dichas metodologías no cubran plenamente alguno de los requisitos, las metodologías definidas en el CRTV y complementarias, en función del tipo de producto evaluado.

Explicación del requisito

El organismo deberá demostrar que:

- Las metodologías técnicas utilizadas en el ámbito RED, solas o complementadas, cubren de forma suficiente los atributos del Anexo I parte I del CRA (seguridad por diseño, seguridad por defecto, resistencia frente a ataques, configuración segura y gestión criptográfica cuando proceda).
- En caso de que las metodologías previamente acreditadas no cubran plenamente alguno de dichos atributos, el organismo ha definido y aplicado extensiones, refinamientos o métodos complementarios, alineados con las referencias del CRTV.
- Las metodologías empleadas permiten documentar la trazabilidad entre el requisito del Anexo I parte I, el método técnico utilizado para su evaluación y el resultado obtenido, garantizando continuidad metodológica respecto a la acreditación RED.
- El organismo utiliza referencias técnicas del CRTV (por ejemplo: ISO/IEC 15408/18045, EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 cuando aplique) como marco técnico de referencia, ya sea integrándolas en sus metodologías existentes o utilizándolas como complemento, cuando resulten aplicables.

Trazabilidad en este documento

- 4.1.1 (requisitos técnicos del producto).
- Matriz 4.4, fila 4 (Capacidad para evaluar requisitos esenciales de seguridad del producto).

Trazabilidad normativa

- CRA: art. 6 y Anexo I parte I.
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, ISO/IEC 15408/18045, IEC 62443 y EN 18031 (estas tres últimas cuando resulten aplicables).

5.2.3.2 Requisito RED-TEC-2 — Evaluación de procesos del fabricante definidos por el Anexo I parte II del CRA**Definición del requisito**

El organismo previamente acreditado conforme al esquema RED DA debe evaluar los procesos del fabricante relacionados con el ciclo de vida seguro del producto, la gestión de vulnerabilidades y la provisión de actualizaciones de seguridad, demostrando que las metodologías de auditoría que aplica en el marco RED permiten evaluar los requisitos del Anexo I parte II del CRA o que, cuando sea necesario, han sido complementadas para cubrir dichos requisitos.

Explicación del requisito

El organismo deberá demostrar que:

- Aplica como base metodologías de auditoría previamente acreditadas en el marco RED para la evaluación de los procesos del fabricante y que dichas metodologías son aplicables a los requisitos del Anexo I parte II del CRA.
- Ha identificado explícitamente las posibles diferencias o lagunas entre:
 - los procesos evaluados en el marco RED, y
 - los requisitos específicos del Anexo I parte II del CRA.
- Ha definido y aplica metodologías o criterios complementarios, basados en referencias técnicas del CRTV (por ejemplo, ISO/IEC 29147 e ISO/IEC 30111), cuando las metodologías RED no cubren plenamente alguno de los aspectos exigidos por el CRA.
- Evalúa de forma efectiva los procesos del fabricante relativos, al menos, a:
 - gestión de vulnerabilidades,
 - ciclo de vida seguro del producto,
 - actualizaciones de seguridad,
 - control de versiones y configuración,
 - gestión de dependencias relevantes para la seguridad.
- Revisa evidencias reales del fabricante, tales como registros de gestión de vulnerabilidades, evidencias de actualizaciones de seguridad, control de configuración y documentación del ciclo de vida, asegurando coherencia con las prácticas evaluativas acreditadas bajo RED DA.
- Documenta la trazabilidad entre los requisitos del Anexo I parte II del CRA, los procesos evaluados, las metodologías aplicadas (RED y/o complementarias) y las conclusiones alcanzadas.

Trazabilidad en este documento

- 4.1.1 (requisitos técnicos del producto).
- Matriz 4.4, fila 5 (Capacidad para evaluar procesos del fabricante).

Trazabilidad normativa - CRA: art. 6 y Anexo I parte II. - CRTV: ISO/IEC 29147, ISO/IEC 30111, IEC 62443, EN 18031, EN 17640 y ETSI EN 303 645 (estas cuatro últimas cuando resulten aplicables).

5.2.3.3 Requisito RED-TEC-3 — Revisión del expediente técnico CRA

Definición del requisito

El organismo debe poder revisar de forma completa y sistemática el expediente de evaluación CRA exigido por el artículo 31 y el Anexo VII del CRA.

Explicación del requisito

El organismo deberá garantizar que:

- Revisa de manera sistemática la documentación técnica exigida por el CRA (arquitectura, diseño, análisis de riesgos, resultados de pruebas, dependencias, manuales y documentación del ciclo de vida), independientemente de que dicha documentación haya sido generada previamente en el marco RED.
- La revisión del expediente CRA no se limita a la documentación existente bajo RED, sino que cubre la totalidad de los elementos exigidos por el Anexo VII del CRA.
- Se mantienen bajo control documental los registros resultantes de la revisión y evaluación CRA, de acuerdo con el sistema de gestión del organismo y con las obligaciones de conservación de registros.
- Dispone de listas de verificación o herramientas equivalentes específicas CRA, que permiten documentar la trazabilidad entre los requisitos aplicables y la documentación revisada.

Trazabilidad en este documento

- 4.2.1 (revisión documental).
- 4.3.1 (SGC operativo).
- Matriz 4.4, fila 6.

Trazabilidad normativa

- CRA: art. 31, Anexo VII.
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031 (estas dos últimas resulte pertinente).

5.2.3.4 Requisito RED-TEC-4 — Capacidad para aplicar los módulos CRA

Definición del requisito

El organismo debe demostrar capacidad para aplicar correctamente los módulos CRA del artículo 32 y del anexo VIII.

Explicación del requisito

El organismo deberá garantizar que:

- En el **módulo B** (examen UE de tipo), aplica las metodologías técnicas que tiene acreditadas en el marco RED para la evaluación del producto, complementándolas cuando proceda con referencias del CRTV para cubrir los requisitos del CRA.
- En el **módulo H** (sistema de calidad), evalúa el sistema de calidad del fabricante utilizando las metodologías de auditoría acreditadas en el marco RED, comprobando que cubren los requisitos del CRA relativos al ciclo de vida seguro, la gestión de vulnerabilidades, las actualizaciones de seguridad y los procesos internos de control, y aplicando criterios complementarios cuando sea necesario.

Trazabilidad en este documento

- 4.2.2.
- Matriz 4.4, filas 7 y 8.

Trazabilidad normativa

- CRA: art. 32, Anexo VIII.
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111 (estas dos últimas cuando resulten aplicables).

5.2.4 REQUISITOS DE COMPETENCIA DEL OEC POR TIPO DE PRODUCTO**5.2.4.1 Requisito RED-PROD-1 — Competencia técnica por tipo de producto (Anexos III y IV CRA)****Definición del requisito**

El organismo debe demostrar competencia técnica específica para cada tipo de producto CRA incluido en su solicitud de alcance, de acuerdo con los requisitos del Anexo I del CRA y con las familias de productos definidas en los Anexos III y IV.

Explicación del requisito

El organismo deberá garantizar que:

- Identifica explícitamente las familias o tipos de producto CRA incluidos en su solicitud de notificación, de acuerdo con los Anexos III y IV del CRA, indicando para cada uno de ellos el alcance técnico evaluado y su relación con los productos y tecnologías previamente cubiertos en el marco RED.
- Existe una correspondencia clara y justificada entre las capacidades técnicas acreditadas del organismo en el marco RED (por ejemplo, experiencia previa en la evaluación de determinadas tecnologías, dominios o clases de producto) y los tipos de producto CRA para los que se solicita la notificación.
- Dispone de una matriz documentada en la que, para cada tipo de producto CRA solicitado, se identifican:
 - las metodologías técnicas aplicadas en el marco RED y, cuando proceda, las metodologías definidas en el CRTV utilizadas para completar la evaluación,
 - y las competencias, cualificación y experiencia del personal asignado a dichas evaluaciones, de forma que se demuestra que cada tipo de producto CRA cuenta con los métodos y recursos humanos necesarios.
- Dispone de herramientas, equipamiento y plataformas de prueba adecuados para los tipos de producto CRA que evalúa, bien como parte de los medios ya acreditados en el marco RED, bien mediante recursos adicionales incorporados para cubrir los requisitos específicos del CRA.

Trazabilidad en este documento

- 4.1.1, 4.1.2, 4.2.1, 4.3.2.
- Matriz 4.4, filas 4, 5 y 9.

Trazabilidad normativa

- CRA: Anexos I, II, IV.
- CRTV: EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, ISO/IEC 15408/18045, IEC 62443 y EN 18031 (estas tres últimas cuando resulten aplicables).

6. PROCEDIMIENTO DE LA AUTORIDAD NOTIFICANTE PARA LA NOTIFICACIÓN DE ORGANISMOS DE EVALUACIÓN DE LA CONFORMIDAD CRA

Este apartado describe el procedimiento que seguirá la Autoridad Notificante para tramitar la notificación de un Organismo de Evaluación de la Conformidad (OEC) conforme a los artículos 38 a 45 del Reglamento (UE) 2024/2847 (CRA).

El procedimiento es único para cualquier entidad que solicite su notificación CRA, independientemente del esquema o ámbito previo desde el que acceda. La única diferencia entre entidades procedentes de distintos esquemas (RED o EUCC) reside en el alcance de la auditoría de ampliación de alcance de ENAC, tal como se detalla en el apartado 5.

La tramitación del expediente para la notificación CRA solo podrá iniciarse una vez que la entidad haya obtenido una acreditación válida emitida por ENAC frente a este documento, resultado de una auditoría de ampliación de alcance respecto de su acreditación previa.

6.1 ACTORES INVOLUCRADOS EN EL PROCEDIMIENTO Y SUS RESPONSABILIDADES

a) Entidad solicitante

La entidad solicitante es cualquier organismo que desee ser notificado bajo el CRA y que disponga de una acreditación válida conforme al artículo 40 del Reglamento. En este periodo transitorio, puede tratarse de:

- un organismo previamente acreditado ISO/IEC 17065 y notificado como organismo de certificación en EUCC,
- un organismo previamente acreditado ISO/IEC 17065 y notificado en el ámbito RED,

La entidad solicitante es responsable de:

- solicitar a ENAC la ampliación de alcance a este procedimiento transitorio de su acreditación,

- preparar y presentar el expediente de notificación a la Autoridad Notificante,
- aportar evidencias documentales que demuestren el cumplimiento de los requisitos del CRA.

b) ENAC

ENAC es responsable de:

- realizar la auditoría de ampliación de alcance CRA conforme al artículo 40 del CRA,
- evaluar que el organismo cumple los requisitos del artículo 39 CRA mediante los criterios de acreditación aplicables (ISO/IEC 17065 e ISO/IEC 17025),
- emitir el certificado de acreditación para este procedimiento transitorio y el informe de auditoría justificativo,
- facilitar a la Autoridad Notificante la información necesaria que soporte la decisión de designación.

c) Autoridad Notificante

La Autoridad Notificante es responsable de:

- recibir y analizar la solicitud de notificación CRA,
- verificar la validez y alcance de la acreditación para el procedimiento transitorio para la CRA emitida por ENAC,
- comprobar la coherencia formal y la completitud del expediente de notificación,
- dictar la designación nacional conforme a los artículos 42–45 del CRA,
- comunicar la notificación a la Comisión Europea mediante el sistema NANDO.

6.2 REQUISITO PREVIO: ACREDITACIÓN PARA EL PROCEDIMIENTO TRANSITORIO PARA LA CRA MEDIANTE AUDITORÍA DE AMPLIACIÓN DE ALCANCE DE ENAC

Antes de iniciar el procedimiento de notificación, la entidad solicitante debe obtener de ENAC una acreditación según los requisitos de este procedimiento transitorio.

La auditoría verificará los requisitos aplicables según el esquema del organismo, evaluando los establecidos en el apartado 5.1 para organismos EUCC y los del apartado 5.2 para organismos RED.

La Autoridad Notificante no abrirá expediente de notificación sin una acreditación para el procedimiento transitorio para la CRA válida cuyo alcance técnico coincida exactamente con el alcance solicitado para la notificación.

La acreditación para el procedimiento transitorio para la CRA emitida por ENAC constituye la base técnica y jurídica sobre la que la Autoridad Notificante fundamenta la designación y la notificación conforme a los artículos 39–45 del CRA.

6.3 SOLICITUD DE NOTIFICACIÓN

La entidad solicitante presentará ante la Autoridad Notificante una solicitud de notificación que incluya, al menos, la información que se enumera a continuación.

Información legal y administrativa

- Identificación jurídica del organismo.
- Declaración responsable de imparcialidad y ausencia de conflictos de interés.
- Datos de contacto oficiales para comunicaciones con la Autoridad Notificante y la Comisión.

La Autoridad Notificante podrá solicitar los documentos societarios (escrituras, estatutos o equivalentes) necesarios para verificar la identidad jurídica y forma legal del organismo, conforme a la LPAC y a los artículos 39 y 42–45 del CRA.

Información organizativa

- Organigrama actualizado del organismo, que refleje claramente la estructura organizativa, las funciones asignadas y la separación efectiva entre las actividades de evaluación y los procesos de toma de decisiones, de acuerdo con los requisitos de imparcialidad aplicables.
- Políticas documentadas de imparcialidad y confidencialidad, que garanticen la independencia de las actividades de evaluación y decisión, así como la protección de la información sensible gestionada por el organismo.
- Descripción del modelo organizativo aplicado con anterioridad en EUCC o RED, que permita evidenciar los roles internos existentes y la separación funcional entre las actividades de evaluación, revisión y decisión.

Información técnica

- Categorías de productos CRA (Anexos II y IV) para las que se solicita notificación.
- Módulos CRA solicitados (B, C, H).
- El organismo debe aportar un documento breve que explique, de forma clara y trazable, cómo sus procedimientos CRA, su personal, las referencias técnicas del CRTV y el alcance solicitado encajan entre sí y permiten realizar evaluaciones conformes al CRA.

Información sobre personal

- Matriz de competencias CRA que permita verificar que, para cada tipo de producto y módulo CRA incluido en el alcance, el organismo dispone de personal con competencias, experiencia y funciones claramente definidas y adecuadas.
- Formación y experiencia demostrada del personal asignado, incluyendo registros de formación relevante en CRA y CRTV, experiencia previa en evaluación de productos y procesos de ciberseguridad, y participación en evaluaciones comparables al alcance solicitado.

Información sobre subcontratación

- Acuerdos de subcontratación, cuando proceda, que identifiquen las actividades subcontratadas, las responsabilidades de las partes y los requisitos aplicables, así como los mecanismos establecidos por el organismo para la supervisión, control y responsabilidad última de las actividades subcontratadas.

acreditación para el procedimiento transitorio para la CRA emitida por ENAC

- Certificado de acreditación para el documento transitorio para la CRA.
- Informe técnico de evaluación emitido por ENAC.

6.4 TRAMITACIÓN DEL EXPEDIENTE POR LA AUTORIDAD NOTIFICANTE

La Autoridad Notificante tramitará la solicitud de notificación presentada por el Organismo de Evaluación de la Conformidad (OEC) de acuerdo con las siguientes actuaciones:

0. Apertura del expediente de notificación CRA

La Autoridad Notificante, una vez recibida la solicitud de notificación presentada por el Organismo de Evaluación de la Conformidad, procederá a la apertura formal del expediente de notificación. A tal efecto, incorporará al expediente toda la documentación aportada por el solicitante, incluyendo la solicitud, la acreditación para el procedimiento transitorio para la CRA emitida por ENAC, la declaración del alcance solicitado, la información sobre subcontratación y cualesquiera otros documentos exigidos por el CRA, por el sistema de acreditación aplicable y por el propio procedimiento de notificación.

1. Verificación administrativa inicial

La Autoridad Notificante comprobará la integridad y validez formal de la solicitud, verificando que el expediente presentado incluye la documentación exigida por el Reglamento (UE) 2024/2847 (CRA), por el sistema de acreditación aplicable y por el propio procedimiento de notificación. Esta verificación se limita a aspectos administrativos y jurídicos, tales como la identificación del organismo solicitante, la declaración del alcance CRA solicitado, la acreditación para el procedimiento transitorio para la CRA aportada, la información sobre subcontratación y las declaraciones y compromisos exigidos, sin entrar en la evaluación técnica de las capacidades del organismo, que corresponde al ámbito de la acreditación.

2. Verificación técnica basada en la acreditación de ENAC

La Autoridad Notificante validará que el organismo ha sido acreditado por ENAC para las actividades CRA solicitadas, confirmando que el alcance de la acreditación cubre los módulos y tipos de producto declaradas por el organismo. Esta verificación se realizará sobre la base de los resultados de la evaluación efectuada por ENAC, sin duplicar ni sustituir la evaluación técnica propia del sistema de acreditación, y en aplicación del principio de presunción de conformidad previsto en el artículo 40 del CRA.

3. Emisión de la designación

Una vez verificado el cumplimiento de los requisitos administrativos y la adecuación de la acreditación para el procedimiento transitorio para la CRA, la Autoridad Notificante emitirá la decisión de designación del organismo. Dicha decisión definirá de forma expresa el alcance autorizado, incluyendo los módulos de evaluación de la conformidad aplicables, los tipos de producto cubiertos y, cuando proceda, las condiciones o limitaciones asociadas a la designación.

4. Notificación a la Comisión Europea

La Autoridad Notificante procederá a la notificación del organismo designado a la Comisión Europea a través del sistema NANDO, incorporando la información exigida por el CRA.

5. Comunicación al organismo

Finalmente, la Autoridad Notificante comunicará formalmente al organismo su notificación como Organismo Notificado CRA, confirmando el alcance autorizado y recordando las obligaciones que le corresponden en su condición de organismo notificado, incluidas las relativas a mantenimiento de la acreditación, gestión de cambios, notificación a la Autoridad Notificante y cooperación con las autoridades competentes.

6.5 RESULTADO DEL PROCEDIMIENTO

La designación del organismo como Organismo de Evaluación de la Conformidad CRA se formaliza mediante decisión de la Autoridad Notificante, previa verificación de la acreditación para el procedimiento transitorio para la CRA válida emitida por ENAC y de la conformidad del expediente de notificación.

La notificación surtirá efectos desde su publicación en el sistema NANDO. Únicamente a partir de dicho momento el organismo podrá ejercer como Organismo Notificado CRA dentro del alcance autorizado.

7. ACTUALIZACIÓN Y TRANSICIÓN FUTURA

La Autoridad Notificante actualizará esta metodología cuando se publiquen normas armonizadas CRA, existan especificaciones comunes CRA, se adopten oficialmente estándares horizontales y verticales CRA o se identifiquen esquemas europeos de certificación como presunción de conformidad CRA. Hasta entonces, ENAC puede emplear este documento como referencia estable para la actividad de acreditación para el procedimiento transitorio para la CRA durante el periodo transitorio.

ANEXOS

INTRODUCCIÓN

Los anexos del presente documento proporcionan orientaciones técnicas y operativas relativas a la aplicación de los distintos módulos de evaluación de la conformidad previstos en el artículo 32 y en el Anexo VIII del CRA. Su finalidad es apoyar una interpretación homogénea y una verificación consistente de las capacidades de los Organismos de Evaluación de la Conformidad (OEC) durante el periodo transitorio descrito en este procedimiento.

Estos anexos tienen carácter informativo y no normativo. No introducen requisitos adicionales a los establecidos en el CRA ni sustituyen a las disposiciones legales, a las normas horizontales de acreditación ni a los procedimientos de ENAC.

En este contexto, únicamente los módulos B (Examen UE de tipo) y H (Garantía total de calidad) implican actividades directas del OEC y son, por tanto, objeto de verificación en el marco del presente procedimiento.

Los módulos A (control interno de la producción) y C (conformidad con el tipo), aun formando parte del sistema de evaluación de la conformidad del CRA, no implican por sí mismos actividades evaluadoras autónomas por parte del OEC en el ámbito de este procedimiento. En particular, el Módulo A corresponde íntegramente al fabricante, mientras que el Módulo C se limita a la verificación de la conformidad de la producción con un tipo previamente evaluado y no constituye, en la práctica, un ámbito independiente de evaluación para el organismo notificado.

No obstante, la referencia a dichos módulos se mantiene en el presente documento, incluidos los anexos correspondientes, por razones de coherencia regulatoria y técnica. En primer lugar, porque forman parte de la arquitectura global del sistema de evaluación de la conformidad del CRA y son necesarios para comprender la relación entre los distintos módulos, en particular la interacción entre los módulos B, C y H. En segundo lugar, porque la documentación y los controles generados en el marco del Módulo A, así como los elementos asociados al Módulo C, pueden ser objeto de revisión indirecta por parte del OEC en el contexto de otros módulos en los que sí interviene directamente, como el Módulo B o el Módulo H. Finalmente, su inclusión permite delimitar de forma explícita las responsabilidades del fabricante y del organismo notificado, evitando interpretaciones erróneas sobre el alcance de la acreditación y de las actividades del OEC.

En consecuencia, los anexos A y C tienen exclusivamente un carácter explicativo y contextual, orientado a facilitar la comprensión del sistema CRA y la correcta integración de los módulos en los que sí interviene el OEC, sin constituir en ningún caso requisitos evaluables en el marco de la acreditación para el procedimiento transitorio.

En los anexos se hace referencia, cuando resulta útil desde el punto de vista explicativo, a funciones y modelos organizativos que distinguen entre organismo de certificación (CB) y entidades técnicas de evaluación, como los ITSEF. Estas referencias reflejan el

funcionamiento habitual de determinados esquemas previos, en particular el esquema EUCC, y se utilizan con carácter ilustrativo para describir la separación funcional entre evaluación técnica, revisión independiente y adopción de decisiones.

Estas referencias no deben interpretarse como la imposición de un modelo organizativo concreto. En el caso de organismos procedentes del ámbito de la Directiva 2014/53/UE (RED) u otros contextos, las actividades técnicas descritas podrán ser realizadas por el propio organismo, por unidades internas diferenciadas o mediante subcontratación conforme al artículo 41 del CRA y a las normas de acreditación aplicables, siempre que se garantice la competencia técnica, la separación funcional, la revisión independiente y la responsabilidad final del organismo.

Las orientaciones contenidas en los anexos deben interpretarse de forma coherente con:

- los requisitos generales del capítulo 4;
- los requisitos específicos verificados en el capítulo 5;
- y la matriz 4.4, que actúa como elemento central de trazabilidad.

Los anexos no pretenden establecer listas cerradas de comprobación ni modelos organizativos obligatorios, sino facilitar una aplicación consistente, proporcionada y técnicamente fundamentada del sistema de evaluación de la conformidad del CRA en ausencia de normas armonizadas o especificaciones comunes.

ANEXO A — MÓDULO A Y SU IMPACTO EN LA ACREDITACIÓN DEL OEC

A.1. OBJETO Y ALCANCE DEL ANEXO

El presente anexo tiene por objeto aclarar el papel del Módulo A (Control interno de la producción) en el contexto del procedimiento transitorio establecido en este documento y precisar su impacto, directo e indirecto, en la acreditación para el procedimiento transitorio para la CRA de los Organismos de Evaluación de la Conformidad (OEC).

Dado que el Módulo A es un módulo de autocontrol del fabricante, este anexo no define actividades evaluadoras autónomas del OEC, sino que tiene una función informativa, destinado a evitar interpretaciones erróneas sobre el alcance de la acreditación y sobre la integración del Módulo A en el sistema global de evaluación de la conformidad del CRA.

A.2. NATURALEZA DEL MÓDULO A EN EL CRA

El Módulo A es un módulo de evaluación de la conformidad basado en el control interno de la producción, en el que la conformidad del producto con los requisitos del CRA se declara bajo la exclusiva responsabilidad del fabricante.

En este módulo no interviene ningún organismo notificado, no se emiten certificados por parte del OEC y no se realiza una evaluación de la conformidad por un tercero. La

función del Módulo A se limita, por tanto, a establecer un marco de autocontrol por parte del fabricante conforme a lo dispuesto en el artículo 32 y en el Anexo VIII del CRA.

A.3. PAPEL DEL OEC RESPECTO AL MÓDULO A

El OEC no aplica el Módulo A, no evalúa técnicamente el producto en el marco de dicho módulo ni adopta decisiones de conformidad asociadas al mismo. En consecuencia, el Módulo A no constituye, por sí mismo, un ámbito de actividad acreditable ni un objeto de verificación independiente en el marco de este procedimiento para un organismo notificado CRA.

No obstante, el OEC debe comprender adecuadamente el alcance y los límites del Módulo A, ya que la documentación técnica y los registros generados por el fabricante en este contexto pueden resultar relevantes en otros procedimientos de evaluación de la conformidad. En particular, dicha documentación puede ser revisada indirectamente en el marco del Módulo B, durante auditorías del Módulo H, o al evaluar la coherencia y completitud global del expediente CRA.

Esta revisión indirecta no implica en ningún caso la evaluación del Módulo A como tal, sino la utilización de la documentación generada por el fabricante como parte de la base técnica para la aplicación de otros módulos en los que sí interviene el OEC.

A.4. CAPACIDADES ESPERABLES DEL OEC RELACIONADAS CON EL MÓDULO A

En el contexto de la acreditación para el procedimiento transitorio para la CRA, ENAC podrá verificar que el OEC comprende correctamente la naturaleza del Módulo A y sus implicaciones, dispone de procedimientos internos que le permitan revisar documentación CRA generada por el fabricante bajo este módulo cuando resulte pertinente y no asume funciones que el CRA reserva expresamente al fabricante.

Estas capacidades no implican la aplicación del Módulo A por parte del OEC, sino la correcta delimitación de responsabilidades y la integración coherente del Módulo A en el conjunto de procedimientos CRA que sí requieren intervención del organismo notificado.

A.5. RELACIÓN CON OTROS MÓDULOS

El Módulo A puede coexistir con los Módulos B, C o H, según el esquema de evaluación de la conformidad aplicable al producto. Su utilización no exime de la aplicación de otros módulos cuando el CRA lo requiera y no altera la responsabilidad del OEC respecto de aquellos módulos cuya aplicación sí le corresponde, conforme al artículo 32 del CRA.

ANEXO B — ORIENTACIONES PARA LA VERIFICACIÓN DE CAPACIDADES DEL OEC EN LA APLICACIÓN DEL MÓDULO B DEL CRA

B.1. OBJETO Y NATURALEZA DEL ANEXO

El presente anexo tiene por objeto proporcionar orientaciones técnicas y operativas para apoyar la verificación de las capacidades de los Organismos de Evaluación de la Conformidad (OEC) que solicitan una ampliación de alcance de su acreditación que cubra CRA para la aplicación del Módulo B (Examen UE de tipo), conforme al artículo 32 y al Anexo VIII del Reglamento (UE) 2024/2847 (CRA).

Este anexo tiene carácter informativo y no normativo. No introduce requisitos adicionales a los establecidos en el CRA ni sustituye a las disposiciones legales, a las normas horizontales de acreditación ni a los procedimientos de ENAC. Su finalidad es facilitar una interpretación homogénea de las capacidades técnicas, organizativas y funcionales que se derivan del marco CRA durante el periodo transitorio.

B.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA

La aplicación del Módulo B se fundamenta en el artículo 32 y en el Anexo VIII del CRA, así como en los artículos 39 y 41 relativos a los requisitos aplicables a los organismos notificados y a la subcontratación. Resultan igualmente de aplicación las normas horizontales de acreditación, en particular ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025, junto con el Reglamento (CE) 765/2008.

Desde el punto de vista técnico, la evaluación en el Módulo B puede hacer uso, cuando resulte pertinente según el tipo de producto, de las referencias incluidas en el Conjunto de Referencias Técnicas Verificables (CRTV), tales como ISO/IEC 15408/18045, EN 17640, ETSI EN 303 645, ISO/IEC 29147, ISO/IEC 30111, IEC 62443 y EN 18031, cuando resulte aplicable según el tipo de producto.

B.3. NATURALEZA DEL MÓDULO B EN EL CRA

El Módulo B es un procedimiento de evaluación de la conformidad mediante el cual el OEC evalúa si un tipo representativo de producto cumple los requisitos esenciales de ciberseguridad establecidos en el Anexo I del CRA. Esta evaluación se centra en el diseño y la arquitectura del producto, en las medidas de seguridad implementadas y en la resistencia frente a ataques, así como en la coherencia entre el producto evaluado, la documentación técnica y los requisitos CRA aplicables.

El resultado del Módulo B es la adopción de una decisión de conformidad sobre el tipo de producto, documentada mediante la emisión del correspondiente certificado de examen UE de tipo por parte del organismo notificado.

Esta evaluación se enmarca en el sistema global de evaluación de la conformidad del CRA, en coherencia con otros módulos aplicables y con la documentación técnica del producto.

B.4. REPARTO DE RESPONSABILIDADES ENTRE CB E ITSEF

La responsabilidad final de la aplicación del Módulo B corresponde al organismo de certificación (CB) que actúa como OEC notificado CRA. El CB es responsable de revisar de forma independiente y crítica los resultados de la evaluación técnica, verificar que la evaluación cubre todos los requisitos aplicables del Anexo I del CRA, adoptar la decisión de conformidad sobre el tipo de producto y emitir el certificado de examen UE de tipo. Estas funciones forman parte de las obligaciones establecidas en el artículo 39 del CRA y en la acreditación conforme a ISO/IEC 17065 y no pueden delegarse.

De conformidad con el artículo 41 del CRA, el CB podrá apoyarse en entidades subcontratadas, como ITSEF u otras unidades técnicas, para la realización de actividades técnicas de evaluación. Dichas actividades pueden incluir análisis detallados de diseño y arquitectura, evaluaciones de vulnerabilidades, pruebas técnicas y la elaboración de informes técnicos de evaluación. Las entidades subcontratadas no adoptan decisiones de conformidad ni emiten certificados y actúan siempre bajo la responsabilidad del CB.

B.5. CAPACIDADES MÍNIMAS ESPERABLES DEL OEC PARA EL MÓDULO B

A efectos de la acreditación para el procedimiento transitorio para la CRA, ENAC podrá verificar que el OEC dispone de metodologías documentadas para evaluar los requisitos del Anexo I parte I del CRA y utiliza de forma adecuada las referencias técnicas del CRTV definidas en el apartado 3.2, aplicándolas de forma proporcionada en función del tipo de producto y del contexto tecnológico. Asimismo, se verificará que el organismo es capaz de integrar de manera coherente los resultados de pruebas, análisis técnicos y evidencias documentales, y que existe una separación efectiva entre las actividades de evaluación técnica, la revisión independiente y la adopción de decisiones.

El OEC debe demostrar que el Módulo B se encuentra correctamente integrado en su sistema de gestión conforme a ISO/IEC 17065 y que dispone de procedimientos específicos para su aplicación.

B.6. EVIDENCIAS TÍPICAS A VERIFICAR POR ENAC

Sin carácter exhaustivo, la verificación de capacidades del OEC para el Módulo B podrá apoyarse en procedimientos internos específicos, informes técnicos de evaluación, registros de revisión independiente y de adopción de decisiones, certificados de examen UE de tipo emitidos cuando existan, matrices de trazabilidad entre requisitos CRA, métodos, evidencias y conclusiones, así como en la documentación relativa a la subcontratación de actividades técnicas.

B.7. RELACIÓN CON OTROS MÓDULOS Y CON LA DOCUMENTACIÓN CRA

La correcta aplicación del Módulo B debe ser coherente con la revisión de la documentación técnica exigida por el artículo 31 y el Anexo VII del CRA, con la aplicación posterior del Módulo C y con los procedimientos de gestión de cambios que puedan

afectar al tipo aprobado. Asimismo, debe integrarse de forma consistente con los procedimientos de notificación descritos en el capítulo 6 del presente documento.

Asimismo, esta aplicación debe interpretarse de forma coherente con el papel de otros módulos del CRA, en particular aquellos que no implican actuación directa del OEC, pero cuyos resultados pueden integrarse en la evaluación global.

ANEXO C — ORIENTACIONES SOBRE EL MÓDULO C Y SU INTEGRACIÓN EN LA ACTIVIDAD DEL OEC EN EL CRA

C.1. OBJETO Y NATURALEZA DEL ANEXO

El presente anexo tiene por objeto proporcionar orientaciones técnicas para clarificar el papel del Módulo C (Conformidad con el tipo) dentro del sistema de evaluación de la conformidad del CRA y su relación con las actividades del OEC, conforme al artículo 32 y al Anexo VIII del Reglamento (UE) 2024/2847 (CRA).

Este anexo tiene carácter informativo y no normativo. No introduce requisitos adicionales a los establecidos en el CRA ni sustituye a las disposiciones legales, a las normas horizontales de acreditación ni a los procedimientos de ENAC. Su finalidad es facilitar la comprensión de la integración del Módulo C en el sistema global de evaluación de la conformidad durante el periodo transitorio.

C.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA

La aplicación del Módulo C se fundamenta en el artículo 32 y en el Anexo VIII del CRA, así como en los artículos 39 y 41 relativos a los requisitos aplicables a los organismos notificados y a la subcontratación. Resultan igualmente de aplicación las normas horizontales de acreditación, en particular ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025, junto con el Reglamento (CE) 765/2008.

C.3. NATURALEZA DEL MÓDULO C EN EL CRA

El Módulo C es un procedimiento de evaluación de la conformidad mediante el cual se verifica que los productos fabricados en serie mantienen la conformidad con el tipo previamente evaluado y aprobado conforme al Módulo B.

A diferencia del Módulo B, el Módulo C no implica una nueva evaluación del diseño o de la arquitectura del producto. Su objeto es confirmar que la producción en serie se ajusta al tipo aprobado, que no se han introducido cambios no evaluados y que se mantienen las configuraciones, versiones y parámetros de seguridad relevantes desde el punto de vista del CRA.

El Módulo C no constituye un procedimiento de evaluación autónomo equiparable al Módulo B, sino un mecanismo de verificación de la continuidad de la conformidad del producto basado en un tipo previamente evaluado.

C.4. PAPEL DEL OEC EN RELACIÓN CON EL MÓDULO C

En el contexto del presente procedimiento, el Módulo C no implica una actividad evaluadora autónoma por parte del OEC, sino que su aplicación se produce de forma integrada con el Módulo B o como alternativa al mismo en el caso del Módulo H.

No obstante, el OEC puede revisar elementos asociados a la producción (registros, configuraciones, versiones) en el marco de la evaluación global de la conformidad, cuando dichos elementos resulten necesarios para verificar la coherencia con el tipo aprobado o para evaluar el impacto de cambios.

Estas actividades no constituyen una aplicación independiente del Módulo C, sino una extensión de la evaluación realizada en otros módulos en los que el organismo notificado sí interviene directamente.

C.5. INTEGRACIÓN DEL MÓDULO C EN LA EVALUACIÓN DE LA CONFORMIDAD

En el contexto del presente procedimiento, no se verifican capacidades específicas del OEC asociadas exclusivamente al Módulo C.

No obstante, el OEC debe ser capaz de integrar adecuadamente los aspectos asociados a la producción en su evaluación global, en particular en relación con:

- la coherencia con el tipo evaluado en el Módulo B;
- la gestión de cambios que puedan afectar a la conformidad del producto;
- la evaluación del sistema de calidad en el Módulo H cuando resulte aplicable.

Asimismo, el organismo debe garantizar que existe trazabilidad entre el tipo aprobado, la producción y las condiciones de conformidad del producto a lo largo del tiempo.

C.6. EVIDENCIAS ASOCIADAS A LA INTEGRACIÓN DEL MÓDULO C

La revisión de la capacidad del OEC para integrar aspectos de producción en la evaluación de la conformidad podrá apoyarse, entre otras, en:

- procedimientos internos relacionados con el control de versiones y configuraciones;
- evidencias de revisión de cambios que afecten al producto;
- documentación técnica que permita vincular la producción con el tipo aprobado;
- registros de decisiones adoptadas en relación con la conformidad del producto.

Estas evidencias deben interpretarse como parte de la evaluación global del proceso de conformidad y no como elementos asociados a una evaluación independiente del Módulo C.

C.7. RELACIÓN CON OTROS MÓDULOS

La correcta aplicación del Módulo C debe ser coherente con el Módulo B, que constituye la base del tipo aprobado. Alternativamente, cuando el fabricante opte por el Módulo H, este sustituye a la aplicación de los Módulos B y C.

Asimismo, el Módulo C debe integrarse de forma coherente con los procedimientos de gestión de cambios, vigilancia poscertificación y mantenimiento de la conformidad previstos en el CRA y en el presente documento.

En consecuencia, el Módulo C debe interpretarse como un elemento del sistema global de evaluación de la conformidad del CRA, cuya aplicación no constituye por sí misma un ámbito independiente de acreditación para el OEC en el marco del presente procedimiento.

ANEXO H — ORIENTACIONES PARA LA VERIFICACIÓN DE CAPACIDADES DEL OEC EN LA APLICACIÓN DEL MÓDULO H

H.1. OBJETO Y NATURALEZA DEL ANEXO

El presente anexo tiene por objeto proporcionar orientaciones técnicas y operativas para apoyar la verificación de las capacidades del OEC en el marco del proceso de acreditación de los Organismos de Evaluación de la Conformidad (OEC) que solicitan una ampliación de alcance de su acreditación que cubra CRA para la aplicación del Módulo H (Garantía total de calidad), conforme al artículo 32 y al Anexo VIII del Reglamento (UE) 2024/2847 (CRA).

Este anexo tiene carácter informativo y no normativo. No introduce requisitos adicionales a los establecidos en el CRA ni sustituye a las disposiciones legales, a las normas horizontales de acreditación ni a los procedimientos de ENAC. Su finalidad es clarificar, durante el periodo transitorio, las capacidades y evidencias que se derivan de la aplicación del Módulo H y que ya se encuentran implícitas en el marco regulatorio y de acreditación vigente.

H.2. MARCO JURÍDICO Y NORMATIVO DE REFERENCIA

La aplicación del Módulo H se fundamenta en el artículo 32 y en el Anexo VIII del CRA, así como en los artículos 39 y 41 relativos a los requisitos aplicables a los organismos notificados y a la subcontratación, y en los artículos 42 a 45 relativos a la notificación y gestión de cambios. Resultan igualmente de aplicación las normas horizontales de acreditación, en particular ISO/IEC 17065 y, cuando proceda, ISO/IEC 17025, junto con el Reglamento (CE) 765/2008.

Desde el punto de vista técnico, la evaluación en el Módulo H puede recurrir, cuando resulte pertinente, a las referencias técnicas del Conjunto de Referencias Técnicas Verificables (CRTV) como apoyo para interpretar la adecuación técnica de los procesos del fabricante relativos al ciclo de vida seguro, la gestión de vulnerabilidades y las

actualizaciones, sin que dichas referencias constituyan por sí mismas criterios formales de auditoría del sistema de calidad.

H.3. NATURALEZA DEL MÓDULO H EN EL CRA

El Módulo H es un procedimiento de evaluación de la conformidad basado en la auditoría y aprobación del sistema de calidad del fabricante. A diferencia de los Módulos B y C, no se centra en la evaluación de un tipo de producto ni en la verificación de la producción en serie, sino en la evaluación de los procesos y controles internos que garantizan que los productos cumplen de forma continuada los requisitos del CRA.

En el contexto del CRA, el Módulo H implica la evaluación de los procesos del fabricante relacionados con el ciclo de vida seguro del producto, la gestión de vulnerabilidades, las actualizaciones y los cambios, el control de la configuración y de las dependencias, así como la existencia y eficacia de mecanismos internos de control y seguimiento. La conformidad de los productos con los requisitos del CRA se deriva del funcionamiento adecuado del sistema de calidad aprobado.

El Módulo H constituye un procedimiento alternativo a la aplicación combinada de los Módulos B y C.

Esta evaluación debe interpretarse en el contexto del sistema global de evaluación de la conformidad del CRA, en coherencia con la documentación técnica del producto y con los módulos alternativos previstos en el Reglamento.

H.4. RESPONSABILIDAD DEL ORGANISMO DE CERTIFICACIÓN (CB)

La aplicación del Módulo H es responsabilidad exclusiva del organismo de certificación (CB) que actúa como OEC notificado CRA. El CB es el único competente para auditar el sistema de calidad del fabricante, evaluar la adecuación de los procesos del ciclo de vida seguro, aprobar formalmente dicho sistema y adoptar la correspondiente decisión de conformidad.

Estas funciones no pueden delegarse en entidades subcontratadas, deben ejercerse bajo la responsabilidad directa del CB y forman parte de las obligaciones organizativas derivadas del artículo 39 del CRA y de la acreditación conforme a ISO/IEC 17065.

H.5. PAPEL DE LAS ENTIDADES SUBCONTRATADAS

De conformidad con el artículo 41 del CRA, el CB podrá apoyarse en entidades subcontratadas para la realización de actividades técnicas auxiliares, tales como análisis técnicos específicos de procesos o controles, revisión de evidencias técnicas concretas, evaluación de aspectos técnicos del ciclo de vida del producto o elaboración de informes técnicos de apoyo.

En ningún caso las entidades subcontratadas podrán auditar o aprobar el sistema de calidad del fabricante, adoptar decisiones de conformidad CRA ni asumir

responsabilidad frente a la Autoridad Notificante. La responsabilidad final de la aplicación del Módulo H recae siempre en el CB.

H.6. CAPACIDADES MÍNIMAS ESPERABLES DEL CB PARA EL MÓDULO H

A efectos de la acreditación para el procedimiento transitorio para la CRA, se podrá verificar que el CB dispone de recursos humanos, organizativos y metodológicos suficientes para la correcta aplicación del Módulo H. Ello incluye personal competente en auditoría de sistemas de calidad y en la evaluación de procesos de ciclo de vida seguro, así como una separación efectiva entre las actividades de evaluación, la revisión independiente y la adopción de decisiones.

Asimismo, el CB dispone de procedimientos documentados específicos para la auditoría del sistema de calidad del fabricante, la revisión y aprobación de dicho sistema, y el seguimiento, vigilancia y gestión de cambios. El Módulo H debe estar integrado de forma coherente en el sistema de gestión del organismo conforme a ISO/IEC 17065.

H.7. EVIDENCIAS TÍPICAS A VERIFICAR POR ENAC

Sin carácter exhaustivo, la verificación de la capacidad del OEC para aplicar el Módulo H podrá apoyarse en procedimientos internos específicos, planes y programas de auditoría del sistema de calidad del fabricante, informes de auditoría reales o simulados, registros de revisión independiente y adopción de decisiones, documentación relativa a la gestión de subcontratación y matrices de competencias del personal implicado.

H.8. RELACIÓN CON OTROS MÓDULOS Y CON LA NOTIFICACIÓN CRA

La aplicación del Módulo H debe ser coherente con la revisión de la documentación técnica exigida por el artículo 31 del CRA y con los procedimientos de notificación, vigilancia y gestión de cambios descritos en los capítulos 4, 5 y 6 del presente documento.

Cuando se utilice el Módulo H como procedimiento de evaluación de la conformidad, este sustituye a la aplicación de los Módulos B y C, de acuerdo con lo previsto en el Anexo VIII del CRA.

REFERENCIAS

LEGISLACIÓN DE LA UNIÓN EUROPEA

- **Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo**, de 23 de octubre de 2024, sobre los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Cyber Resilience Act – CRA).
- **Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del 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.
- **Decisión n.º 768/2008/CE del Parlamento Europeo y del Consejo**, de 9 de julio de 2008, relativa a un marco común para la comercialización de los productos (Nuevo Marco Legislativo – NLF).
- **Directiva 2014/53/UE del Parlamento Europeo y del Consejo**, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos (RED).
- **Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo**, de 17 de abril de 2019, relativo a ENISA y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Cybersecurity Act).
- **Reglamento de Ejecución (UE) 2024/482 de la Comisión**, por el que se establecen las disposiciones de aplicación del Reglamento (UE) 2019/881 en lo relativo al esquema europeo de certificación de la ciberseguridad basado en los criterios comunes (EUCC).

NORMAS HORIZONTALES DE ACREDITACIÓN Y EVALUACIÓN DE LA CONFORMIDAD

- **ISO/IEC 17065** — Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.
- **ISO/IEC 17025** — Requisitos generales para la competencia de los laboratorios de ensayo y calibración.
- **ISO/IEC 17020** — Evaluación de la conformidad. Requisitos para el funcionamiento de diferentes tipos de organismos que realizan inspección (cuando resulte aplicable).

NORMAS TÉCNICAS INCLUIDAS EN EL CONJUNTO DE REFERENCIAS TÉCNICAS VERIFICABLES (CRTV)

- **ISO/IEC 15408 (todas las partes)** — Tecnologías de la información. Técnicas de seguridad. Criterios de evaluación de la seguridad TI (Common Criteria).
- **ISO/IEC 18045** — Metodología para la evaluación de la seguridad de productos de tecnologías de la información.
- **EN 17640** Fixed-time cybersecurity evaluation methodology for ICT products (FiT CEM).

- **ETSI EN 303 645** — Ciberseguridad para dispositivos IoT de consumo: requisitos básicos (cuando resulte aplicable según el tipo de producto).
- **ISO/IEC 29147** — Técnicas de seguridad. Divulgación de vulnerabilidades.
- **ISO/IEC 30111** — Técnicas de seguridad. Procesos de tratamiento de vulnerabilidades.
- **IEC 62443** — Redes de comunicación industrial – Seguridad de redes y sistemas.
- **EN 18031** — Requisitos de seguridad para equipos radioeléctricos.

DOCUMENTACIÓN EUROPEA SOBRE EL ESQUEMA EUCC Y LA ACREDITACIÓN DE ORGANISMOS

- **ENISA, EUCC** — *Accreditation of Certification Bodies*
- **ENISA, EUCC** — *Accreditation of IT Security Evaluation Facilities (ITSEFs)*
- **ENISA, EUCC** *Guidelines on the Authorisation of Conformity Assessment Bodies.*

REFERENCIAS INTERNAS AL CRA

- **Anexo I del CRA** — Requisitos esenciales de ciberseguridad.
- **Anexo VII del CRA** — Documentación técnica.
- **Anexo VIII del CRA** — Procedimientos y módulos de evaluación de la conformidad (Módulos A, B, C y H).

Nota sobre la vigencia de las referencias Las normas, estándares y documentos técnicos citados en esta sección se entenderán referidos a su versión vigente en el momento de la evaluación, acreditación o auditoría correspondiente, salvo que se indique expresamente lo contrario.