2025/2540

12.12.2025

REGLAMENTO DE EJECUCIÓN (UE) 2025/2540 DE LA COMISIÓN

de 9 de diciembre de 2025

por el que se establecen disposiciones de aplicación del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo en lo que respecta al establecimiento de un plan para las revisiones interpares

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 (en lo sucesivo, «Reglamento sobre la Ciberseguridad») ([1]), y en particular su artículo 59, apartado 5,

Considerando lo siguiente:

(1) De conformidad con el artículo 59, apartado 4, del Reglamento (UE) 2019/881, las revisiones interpares de las autoridades nacionales de certificación de la ciberseguridad deben llevarlas a cabo dos de estas autoridades de otros Estados miembros y la Comisión. Con vistas a lograr normas equivalentes con respecto a los certificados europeos de ciberseguridad y las declaraciones de conformidad de la UE, la Comisión debe supervisar los aspectos relacionados con el cumplimiento del presente Reglamento y garantizar que las revisiones interpares se lleven a cabo de manera coherente en toda la Unión. Con el fin de ayudar a identificar las buenas prácticas, los retos y las lecciones aprendidas de la aplicación de los esquemas europeos de certificación de la ciberseguridad, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) debe tener la oportunidad de participar en las revisiones interpares en calidad de observador. Para apoyar la aplicación armonizada de las disposiciones del presente Reglamento, la ENISA, en cooperación con la Comisión y el Grupo Europeo de Certificación de la Ciberseguridad (GECC), también debe poder elaborar plantillas.

(2) Con el fin de garantizar una planificación previsible y una asignación eficiente de los recursos, las revisiones interpares de cada autoridad nacional de certificación de la ciberseguridad deben llevarse a cabo de conformidad con un calendario establecido. Debe ser posible que una autoridad nacional de certificación de la ciberseguridad solicite retrasar su revisión interpares en circunstancias excepcionales, como escasez inesperada de personal o casos de fuerza mayor. A tal efecto, es necesario establecer las modalidades de evaluación de dicha solicitud, garantizando que se mantenga el calendario general y que los objetivos del mecanismo de revisión interpares no se vean comprometidos.

(3) Con el fin de garantizar que todos los Estados miembros contribuyan a la aplicación del mecanismo de revisión interpares, así como de permitirles beneficiarse del aprendizaje entre iguales, las autoridades nacionales de certificación de la ciberseguridad de cada Estado miembro deben llevar a cabo dos revisiones interpares a lo largo de un período de cinco años. Por lo tanto, debe establecerse un sistema de rotación que permita a las autoridades nacionales de certificación de la ciberseguridad de todos los Estados miembros organizar su participación. También es necesario establecer los criterios que las autoridades nacionales de certificación de la ciberseguridad deben tener en cuenta a la hora de seleccionar a los representantes para llevar a cabo las revisiones interpares, con el objetivo de garantizar unos conocimientos especializados y unas competencias adecuados. También debe permitirse que las autoridades nacionales de certificación de la ciberseguridad participen en las revisiones interpares en calidad de observadores, con el fin de supervisar y aprender del proceso. En tales casos, no debe exigirse que su representante tenga los mismos conocimientos y competencias que se espera de los representantes de las autoridades nacionales de certificación de la ciberseguridad que lleven a cabo las revisiones interpares.

(4) Con el fin de garantizar que una autoridad nacional de certificación de la ciberseguridad sea objeto de una revisión interpares por parte de al menos una autoridad nacional de certificación de la ciberseguridad que aplique el mismo enfoque para la expedición de certificados de nivel «elevado», la ENISA debe indicar, al invitar a las autoridades nacionales de certificación de la ciberseguridad a manifestar su interés por ser revisores interpares, si la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares expide directamente certificados de nivel «elevado», utiliza el modelo de aprobación previa a que se refiere el artículo 56, apartado 6, letra a), del Reglamento (UE) 2019/881, concede una delegación general de conformidad con la letra b) de dicho apartado, o combina estas características.

([1]) DO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(5) A fin de garantizar criterios y procedimientos de evaluación comunes para el funcionamiento de las revisiones interpares en toda la Unión, cada revisión interpares debe incluir siempre un cuestionario de autoevaluación, una revisión de la documentación y una visita *in situ*, acompañada de entrevistas. Tras la visita *in situ*, el equipo de revisión interpares debe debatir las conclusiones con la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, preparar un proyecto de informe y presentarlo a la autoridad nacional de certificación de la ciberseguridad objeto de dicha revisión para que formule observaciones, con vistas a garantizar el consenso, en la medida de lo posible. El equipo de revisión interpares debe presentar al GECC el informe final, que puede incluir directrices o recomendaciones para permitir la mejora de la autoridad nacional de control nacional objeto de la revisión interpares. El GECC, a propuesta del equipo de revisión interpares, también debe aprobar un informe sucinto que se pondrá a disposición del público.

(6) A fin de garantizar que la información obtenida a través del proceso de revisión interpares se gestione de manera segura, el equipo de revisión interpares debe garantizar el uso de canales de comunicación seguros, como una plataforma segura para el almacenamiento y el intercambio de documentos, y el uso de las salvaguardias adecuadas para los datos confidenciales compartidos entre los miembros de dicho equipo. La ENISA, teniendo en cuenta las mejores prácticas existentes de las autoridades nacionales de certificación de la ciberseguridad, también debe poder elaborar directrices sobre cómo garantizar una comunicación segura, en particular con vistas a garantizar que el nivel de seguridad aplicado por el equipo de revisión interpares al recopilar, compartir y tratar información esté en consonancia con las necesidades de seguridad de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares.

(7) Con el fin de facilitar la cooperación y el intercambio efectivo de información entre las autoridades nacionales de certificación de la ciberseguridad, el GECC, en particular su subgrupo sobre la revisión interpares, debe contribuir al desarrollo de plantillas y asistir a la Comisión en la aplicación del presente Reglamento.

(8) El mecanismo de revisión interpares constituye un servicio público digital transeuropeo en el sentido del Reglamento (UE) 2024/903 del Parlamento Europeo y del Consejo ([2]). El presente Reglamento introduce nuevos requisitos vinculantes que afectan a dicho servicio y, como tal, está sujeto a la obligación de evaluación de la interoperabilidad en virtud del artículo 3 del Reglamento (UE) 2024/903. En consecuencia, se ha llevado a cabo una evaluación de la interoperabilidad y el informe resultante debe publicarse en el Portal de la Europa Interoperable.

(9) Al elaborar el presente Reglamento, la Comisión ha tenido en cuenta los puntos de vista del GECC, incluido su subgrupo sobre la revisión interpares.

(10) Las medidas previstas en el presente Reglamento se ajustan al dictamen del Comité creado en virtud del artículo 66 del Reglamento (UE) 2019/881.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

Calendario, frecuencia y coste de las revisiones interpares

1. Las revisiones interpares de las autoridades nacionales de certificación de la ciberseguridad se llevarán a cabo de conformidad con el calendario establecido en el anexo I. Cada revisión interpares se completará en la fecha indicada en dicho calendario y, a continuación, se llevará a cabo una vez cada cinco años.

2. En circunstancias excepcionales, la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares podrá presentar a la Comisión una solicitud debidamente justificada para aplazar su revisión interpares más allá de la fecha indicada en el calendario que figura en el anexo I. La Comisión, en cooperación con el Grupo Europeo de Certificación de la Ciberseguridad (GECC) establecido por el artículo 62 del Reglamento (UE) 2019/881, evaluará la solicitud e informará oportunamente del resultado a todas las partes pertinentes.

([2]) Reglamento (UE) 2024/903 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se establecen medidas a fin de garantizar un alto nivel de interoperabilidad del sector público en toda la Unión (Reglamento sobre la Europea Interoperable) (DO L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Cuando un Estado miembro, de conformidad con el artículo 58, apartado 1, del Reglamento (UE) 2019/881, haya designado:

a) más de una autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares en su territorio, todas las autoridades nacionales de certificación de la ciberseguridad de ese Estado miembro serán objeto de una revisión interpares en paralelo;

b) una o varias autoridades nacionales de certificación de la ciberseguridad de otro Estado miembro, esa o esas autoridades nacionales de certificación de la ciberseguridad podrán ser objeto de una revisión interpares de conformidad con el calendario establecido para el Estado miembro que las haya designado o para el Estado miembro de las autoridades nacionales de certificación de la ciberseguridad designadas, en relación con las tareas de supervisión llevadas a cabo en el Estado miembro designador.

4. La Agencia de la Unión Europea para la Ciberseguridad (ENISA) pondrá a disposición del público la siguiente información en el sitio web sobre los esquemas europeos de certificación de la ciberseguridad creados en virtud del artículo 50 del Reglamento (UE) 2019/881:

a) la información sobre el calendario que figura en el anexo I;

b) la lista de las autoridades nacionales de certificación de la ciberseguridad que realicen las revisiones interpares mantenida de conformidad con el artículo 2, apartado 5.

5. Cada autoridad nacional de certificación de la ciberseguridad que participe en el proceso de revisión interpares correrá con sus propios costes de participación.

Artículo 2

Sistema de rotación para las autoridades nacionales de certificación de la ciberseguridad que realicen las revisiones interpares

1. De conformidad con el artículo 59, apartado 4, del Reglamento (UE) 2019/881, cada revisión interpares será llevada a cabo por dos autoridades nacionales de certificación de la ciberseguridad de otros Estados miembros y la Comisión. Las autoridades nacionales de certificación de la ciberseguridad de cada Estado miembro participarán en la revisión interpares de al menos dos autoridades nacionales de certificación de la ciberseguridad durante cada período establecido en el anexo I.

2. Las autoridades nacionales de certificación de la ciberseguridad de otros Estados miembros podrán participar en la revisión interpares en calidad de observadores con uno o varios representantes, con el acuerdo de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares y la Comisión.

3. Un representante de la ENISA podrá participar en la revisión interpares en calidad de observador. También podrán participar otros representantes, con el acuerdo de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares y la Comisión.

4. Los observadores tendrán acceso a la misma información que los demás miembros del equipo de revisión interpares, pero no llevarán a cabo tareas relacionadas con la ejecución de la revisión interpares.

5. La ENISA, en cooperación con la Comisión y el GECC, propondrá y mantendrá la lista de autoridades nacionales de certificación de la ciberseguridad que deben llevar a cabo las revisiones interpares según el calendario establecido en el anexo I. Durante un año determinado, la ENISA, en cooperación con la Comisión, pedirá a las autoridades nacionales de certificación de la ciberseguridad que expresen su interés en llevar a cabo las revisiones interpares previstas en el anexo I para el año siguiente, o en participar como observadores en dichas revisiones.

6. Cuando más de dos autoridades nacionales de certificación de la ciberseguridad manifiesten su interés en llevar a cabo la revisión interpares de la misma autoridad nacional de certificación de la ciberseguridad, la Comisión y la ENISA consultarán a las autoridades nacionales de certificación de la ciberseguridad interesadas y decidirán sobre los participantes en la revisión interpares.

7. Cuando, en un año determinado, no haya suficientes autoridades nacionales de certificación de la ciberseguridad que expresen su interés en llevar a cabo las revisiones interpares, la Comisión, previa consulta al GECC, seleccionará las autoridades nacionales de certificación de la ciberseguridad que llevarán a cabo dichas revisiones. En su selección, la Comisión tendrá en cuenta la obligación de las autoridades nacionales de certificación de la ciberseguridad de cada Estado miembro de participar en la revisión interpares de al menos dos autoridades nacionales de certificación de la ciberseguridad, a que se refiere el apartado 1.

Artículo 3

Criterios sobre la composición del equipo de revisión interpares

1. A su debido tiempo antes del inicio de la revisión interpares, cada una de las autoridades nacionales de certificación de la ciberseguridad que participen en la revisión interpares designará a un representante para llevarla a cabo. Las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares podrán designar a más de un representante cuando sea necesario para garantizar que el equipo de revisión interpares tenga las competencias necesarias para llevar a cabo dicha revisión.

2. Los representantes de las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares, con la excepción de aquellos que participen en calidad de observadores, deberán cumplir los siguientes criterios:

a) tener al menos dos años de experiencia trabajando para la autoridad nacional de certificación de la ciberseguridad o haber participado en al menos dos revisiones interpares en calidad de observadores;

b) poseer conocimientos suficientes del marco de certificación de la ciberseguridad establecido en el Reglamento (UE) 2019/881;

c) tener un buen conocimiento del inglés y, en la medida de lo posible, de una o varias de las lenguas habladas en el Estado miembro de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares;

d) operar con independencia de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares.

3. Las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares velarán por que cualquier riesgo de conflicto de intereses que afecte a los representantes designados se comunique a las demás autoridades nacionales de certificación de la ciberseguridad, a la Comisión y a la ENISA, antes del inicio del proceso de revisión interpares. La autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares podrá oponerse a la designación de representantes concretos de conformidad con el apartado 5.

4. Las autoridades nacionales de certificación de la ciberseguridad que realicen la revisión interpares elegirán entre sí a un representante («jefe de equipo») para coordinar la revisión interpares.

5. La Comisión facilitará a la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares los nombres y datos de contacto de los representantes de las autoridades nacionales de certificación de la ciberseguridad que vayan a realizar la revisión interpares antes del inicio de esta. Cuando la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares desee oponerse a la designación de uno o más representantes, proporcionará, en un plazo de dos semanas, una justificación clara a la Comisión, informará a la ENISA y al GECC y solicitará que la autoridad nacional de certificación de la ciberseguridad que vaya a realizar la revisión interpares designe a un representante diferente.

6. Cuando el procedimiento establecido en el apartado 5 cause retrasos indebidos en la puesta en marcha de la revisión interpares debido a circunstancias excepcionales, la Comisión, en consulta con la ENISA y el GECC, decidirá sobre la composición del equipo de revisión interpares.

Artículo 4

Metodología para la revisión interpares

1. La revisión interpares evaluará los aspectos enumerados en el anexo II, de conformidad con el artículo 59, apartado 3, del Reglamento (UE) 2019/881.

2. La ENISA, en cooperación con el GECC y la Comisión, podrá elaborar plantillas para la evaluación de los procesos establecidos por la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares.

3. La revisión interpares comprenderá lo siguiente:

a) un cuestionario de autoevaluación;

b) una evaluación de la documentación pertinente;

c) entrevistas en línea o físicas, o ambas;

d) una visita *in situ*.

4. La duración de la revisión interpares podrá acordarse previamente entre el equipo de revisión interpares y la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, en función del tamaño y la complejidad de las actividades de esta última. La visita *in situ* no podrá durar más de tres días laborables.

5. Salvo que el equipo de revisión interpares, la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares y la Comisión acuerden otra cosa, la lengua de cooperación será el inglés. El informe de la revisión interpares a que se refiere el artículo 5 se redactará al menos en inglés.

6. La autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares cooperará y facilitará al equipo de revisión interpares acceso a la información y los documentos necesarios para llevar a cabo la revisión interpares. La autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares presentará el cuestionario de autoevaluación y el último informe sucinto anual adoptado de conformidad con el artículo 58, apartado 7, letra g), del Reglamento (UE) 2019/881 al menos 21 días antes de la fecha de la visita *in situ*. Se presentarán documentos adicionales a petición del equipo de revisión interpares en un plazo de siete días a partir de la recepción de dichas solicitudes.

7. Los documentos se facilitarán en inglés, salvo que se acuerde otra cosa de conformidad con el apartado 5. Cuando los documentos no se faciliten en inglés, el equipo de revisión interpares podrá solicitar que los documentos necesarios para llevar a cabo la revisión interpares se traduzcan al inglés.

8. Antes de elaborar el informe de la revisión interpares de conformidad con el artículo 5, el equipo de revisión interpares debatirá las conclusiones preliminares con la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares.

Artículo 5

Informe de la revisión interpares

1. En un plazo de 21 días a partir de la ejecución de la revisión interpares, el equipo de revisión interpares elaborará un proyecto de informe de revisión interpares, que incluirá información detallada sobre el Estado miembro de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, las autoridades nacionales de certificación de la ciberseguridad que hayan realizado dicha revisión, la Comisión y cualquier observador, así como las constataciones y conclusiones de la revisión interpares. Cuando sea necesario, el informe incluirá recomendaciones que permitan la mejora de los aspectos que abarque la revisión interpares.

2. La ENISA, en cooperación con la Comisión y el GECC, podrá elaborar una plantilla para el informe de la revisión interpares.

3. Tras elaborar el proyecto de informe de la revisión interpares de conformidad con el apartado 1, el equipo de revisión interpares lo facilitará a la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares para que formule observaciones en un plazo de 14 días. El equipo de revisión interpares evaluará las observaciones y, en la medida de lo posible, las integrará en el informe final, con vistas a garantizar el consenso. En caso de desacuerdo, la respuesta de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares se adjuntará al informe final.

4. El informe final se enviará al GECC en un plazo de dos meses a partir de la ejecución de la revisión interpares, incluido un resumen para su publicación. De conformidad con el artículo 59, apartado 6, del Reglamento (UE) 2019/881, el GECC analizará el informe y aprobará su resumen, que se publicará en el sitio web sobre los esquemas europeos de certificación de la ciberseguridad creados en virtud del artículo 50 del Reglamento (UE) 2019/881. El resumen incluirá también la respuesta de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, o de partes de la misma, de acuerdo con dicha autoridad.

5. El equipo de revisión interpares anonimizará los datos personales que pueda haber recogido durante la revisión interpares antes de difundir el informe de la revisión interpares a terceros ajenos al equipo de revisión interpares.

Artículo 6

Confidencialidad

1. Todas las partes involucradas en las revisiones interpares respetarán la confidencialidad de la información y los datos obtenidos en el ejercicio de sus funciones y actividades, de modo que se protejan, en particular:

a) los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de las personas físicas o jurídicas, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo ([3]);

b) la aplicación efectiva del presente Reglamento;

c) los intereses públicos y de seguridad nacional;

d) la integridad de las causas penales o los procedimientos administrativos.

2. El equipo de revisión interpares velará por que toda la información obtenida a través del proceso de revisión interpares se gestione de forma segura. Una vez elaborados el informe final y el resumen a que se refiere el artículo 5, apartado 4, el equipo de revisión interpares, incluido cualquier observador, suprimirá o destruirá todos los documentos distintos del informe final y del resumen que se hayan recogido o generado como parte del proceso de revisión interpares.

3. La ENISA, teniendo en cuenta las mejores prácticas existentes de las autoridades nacionales de certificación de la ciberseguridad, podrá, en cooperación con el GECC, elaborar directrices sobre comunicaciones seguras y confidenciales.

([3]) Directiva (UE) 2016/943 del Parlamento Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas (DO L 157 de 15.6.2016, p. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Artículo 7

Creación de capacidades

La ENISA analizará los resultados agregados de las revisiones interpares y pondrá de relieve las lecciones aprendidas y las mejores prácticas, con el fin de contribuir al desarrollo de capacidades para las autoridades nacionales de certificación de la ciberseguridad y al mantenimiento de los esquemas europeos de certificación de la ciberseguridad. Dicho análisis podrá incluir, cuando proceda, formación y directrices adicionales para las autoridades nacionales de certificación de la ciberseguridad, elaboradas en cooperación con el GECC.

Artículo 8

Entrada en vigor

El presente Reglamento entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 9 de diciembre de 2025.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO I

Calendario de las autoridades nacionales de certificación de la ciberseguridad que están sujetas a revisión interpares

Las autoridades nacionales de certificación de la ciberseguridad de los siguientes Estados miembros serán objeto de una revisión interpares a más tardar el 31 de diciembre de 2026 y, a continuación, cada cinco años:

Suecia, Bélgica, Eslovaquia, Alemania, Malta, Chequia

Las autoridades nacionales de certificación de la ciberseguridad de los siguientes Estados miembros serán objeto de una revisión interpares a más tardar el 31 de diciembre de 2027 y, a continuación, cada cinco años:

Hungría, Grecia, Estonia, Eslovenia, Países Bajos, Italia

Las autoridades nacionales de certificación de la ciberseguridad de los siguientes Estados miembros serán objeto de una revisión interpares a más tardar el 31 de diciembre de 2028 y, a continuación, cada cinco años:

Croacia, Dinamarca, Lituania, España, Bulgaria e Irlanda

Las autoridades nacionales de certificación de la ciberseguridad de los siguientes Estados miembros serán objeto de una revisión interpares a más tardar el 31 de diciembre de 2029 y, a continuación, cada cinco años:

Finlandia, Austria, Rumanía, Luxemburgo, Letonia, Polonia

Las autoridades nacionales de certificación de la ciberseguridad de los siguientes Estados miembros y Estados AELC del EEE serán objeto de una revisión interpares a más tardar el 31 de diciembre de 2030 y, a continuación, cada cinco años:

Chipre, Francia, Portugal, Liechtenstein, Noruega, Islandia

ANEXO II

Metodología de la revisión interpares

II.1 Separación entre las actividades de certificación y de supervisión

Al evaluar la separación entre las actividades de certificación y las actividades de supervisión de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares a que se refiere el artículo 59, apartado 3, letra a), del Reglamento (UE) 2019/881, la revisión interpares incluirá, como mínimo, los siguientes aspectos:

a) una descripción detallada del funcionamiento de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares, en la que se identifiquen claramente las diferentes entidades o departamentos que participan en la aplicación del Reglamento (UE) 2019/881;

b) un inventario de las actividades de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares en relación con las actividades enumeradas en el artículo 58, apartado 7, del Reglamento (UE) 2019/881;

c) cuando la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares expida certificados, una explicación que demuestre que no hay interferencia entre sus actividades de certificación y las actividades de supervisión indicadas en la letra b).

II.2 Supervisión y cumplimiento de las normas para controlar la conformidad con los certificados

Al evaluar los procedimientos de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares para supervisar y cumplir las normas destinadas a controlar la conformidad de los productos, servicios y procesos de TIC y los servicios de seguridad gestionados con los certificados europeos de ciberseguridad a que se refiere el artículo 59, apartado 3, letra b), del Reglamento (UE) 2019/881, la revisión interpares evaluará al menos los siguientes aspectos:

a) la calidad y el nivel de detalle de la descripción de dichos procesos y procedimientos y la medida en que están documentados;

b) si dichos procesos y procedimientos abarcan los esquemas europeos de certificación de la ciberseguridad pertinentes, y en qué medida;

c) si la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares está efectivamente facultada para inspeccionar a los organismos de evaluación de la conformidad que expiden certificados y, en caso necesario, para hacer cumplir la retirada de certificados;

d) el grado de cooperación de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares con las autoridades de vigilancia del mercado pertinentes;

e) si la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares dispone de un mecanismo para tramitar las reclamaciones de personas físicas o jurídicas, exigido en virtud del artículo 58, apartado 7, letra f), del Reglamento (UE) 2019/881, incluidas pruebas de si las personas físicas y jurídicas tienen derecho a presentar una reclamación y a obtener una tutela judicial efectiva de conformidad con los artículos 63 y 64 de dicho Reglamento, respectivamente.

II.3 Control y cumplimiento de las obligaciones de los fabricantes o proveedores

Al evaluar los procedimientos de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares para controlar y cumplir las obligaciones de los fabricantes o proveedores que lleven a cabo la autoevaluación de la conformidad, tal como se contempla en el artículo 59, apartado 3, letra c), del Reglamento (UE) 2019/881, la revisión interpares evaluará al menos los siguientes aspectos:

a) si la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares ha establecido tales procedimientos y en qué medida están documentados, en particular si ha establecido un mecanismo para recibir y procesar información de fuentes externas;

b) si dichos procedimientos abarcan los esquemas europeos de certificación de la ciberseguridad pertinentes, y en qué medida;

c) si la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares lleva a cabo sus propias investigaciones, y en qué medida, y si el ámbito de las investigaciones abarca las obligaciones de los fabricantes establecidas en el artículo 53, apartados 2 y 3, del Reglamento (UE) 2019/881 y en los esquemas europeos de certificación de la ciberseguridad correspondientes;

d) si existe un procedimiento para el intercambio de información entre las actividades de certificación y las actividades de supervisión de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares que sean pertinentes para el control y el cumplimiento de las obligaciones de los fabricantes o proveedores.

II.4 **Control, autorización y supervisión de los organismos de evaluación de la conformidad**

Al evaluar los procedimientos de la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares para el control, la autorización y la supervisión de las actividades de los organismos de evaluación de la conformidad a que se refiere el artículo 59, apartado 3, letra d), del Reglamento (UE) 2019/881, la revisión interpares evaluará al menos los siguientes aspectos:

a) la calidad y el nivel de detalle de la descripción de dichos procedimientos y la medida en que están documentados, también para la cooperación con el organismo nacional de acreditación;

b) las estadísticas clave sobre el número de autorizaciones concedidas, suspendidas o retiradas, el número total de organismos de evaluación de la conformidad en activo, el número de certificados expedidos y el número de medidas correctoras adoptadas por la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares;

c) cuando la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares permita la expedición de certificados europeos de ciberseguridad de nivel «elevado» previa aprobación o sobre la base de una delegación general de la tarea establecida en el artículo 56, apartado 6, del Reglamento (UE) 2019/881, los conocimientos especializados del personal y los procedimientos a través de los cuales la autoridad nacional de certificación de la ciberseguridad objeto de la revisión interpares controla y supervisa las actividades de los organismos de evaluación de la conformidad.