Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículos 42 y 43 del Reglamento

Versión 3.0

4 de junio de 2019

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Adoptado

Historial de versiones

Versión 3.0	4 de junio de 2019	Inclusión del anexo 2 (versión 2.0 del anexo 2, adoptado el 4 de junio de 2019 tras la consulta pública)
Versión 2.1	9 de abril de 2019	Adopción de una corrección de errores de las Directrices (párrafo 45)
Versión 2.0	23 de enero de 2019	Adopción de las Directrices después de la consulta pública. En la misma fecha en la que el anexo 2 (versión 1.0) se adoptó para consulta pública
Versión 1.0	25 de mayo de 2018	Adopción de las Directrices para la consulta pública

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, «RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su Protocolo 37, modificado por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018,

Vistos los artículos 12 y 22 de su reglamento interno de 25 de mayo de 2018,

Examinados los resultados de la consulta pública sobre las directrices, que tuvo lugar entre el 30 de mayo de 2018 y el 12 de julio de 2018, y sobre el anexo 2, que tuvo lugar entre el 15 de febrero y el 29 de marzo de 2019, tal y como establece el artículo 70, apartado 4, del RGPD

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1 INTRODUCCIÓN

1. El Reglamento General de Protección de Datos [Reglamento (UE) 2016/279, «el RGPD» o «el Reglamento»], ofrece un marco modernizado de rendición de cuentas y cumplimiento de los derechos fundamentales para la protección de datos en Europa. Un conjunto de medidas que facilitan el cumplimiento de las disposiciones del RGPD constituye el centro de este nuevo marco. Entre ellas se incluyen requisitos obligatorios en circunstancias específicas (como el nombramiento de delegados de protección de datos y la realización de evaluaciones de impacto sobre la protección de datos) y medidas voluntarias como códigos de conducta y mecanismos de certificación.
2. Antes de la adopción del RGPD, el Grupo de Trabajo del Artículo 29 estableció que la certificación podía desempeñar un papel importante en el marco de rendición de cuentas con relación a la protección de datos.1 Con el fin de que la certificación proporcione pruebas fiables del cumplimiento de la protección de datos, debería contarse con normas claras que establezcan los requisitos para la emisión de una certificación.2 El artículo 42 del RGPD establece la base jurídica para la elaboración de dichas normas.
3. El artículo 42, apartado 1, del RGPD establece que:

   «Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el

[1] Grupo de Trabajo del Artículo 29, Dictamen 3/2010 sobre el principio de responsabilidad, WP173, de 13 de julio de 2010, apartados 69 a 71.
[2] Grupo de Trabajo del Artículo 29, Dictamen 3/2010 sobre el principio de responsabilidad, WP173, apartado 69.

cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas».

4. Los mecanismos de certificación3 pueden mejorar la transparencia para los interesados, pero también las relaciones entre empresas, por ejemplo, entre responsables del tratamiento y encargados del tratamiento. El considerando 100 del RGPD dispone que el establecimiento de mecanismos de certificación puede aumentar la transparencia y el cumplimiento del Reglamento y puede permitir a los interesados evaluar el nivel de protección de datos de los productos y servicios correspondientes.4

5. El RGPD no introduce el derecho o la obligación de emitir una certificación por parte de los responsables y los encargados del tratamiento; en lo que respecta al artículo 42, apartado 3, la certificación es un proceso voluntario para contribuir a demostrar el cumplimiento del RGPD. Los Estados miembros y las autoridades de control deben fomentar el establecimiento de mecanismos de certificación y determinarán el compromiso de las partes interesadas en el proceso y el ciclo de vida de la certificación.

6. Asimismo, el cumplimiento de los mecanismos de certificación aprobados es un factor que deben considerar las autoridades de control como agravante o atenuante a la hora de decidir imponer una multa administrativa y de establecer el importe de dicha multa (artículo 83, apartado 2, letra j).5

1.1 Ámbito de aplicación de las directrices

7. Las presentes directrices tienen un ámbito de aplicación limitado; no son un manual de procedimiento para la certificación con arreglo al RGPD. Su objetivo principal es identificar los requisitos y criterios generales que puedan resultar pertinentes para todo tipo de mecanismos de certificación emitidos con arreglo a los artículos 42 y 43 del RGPD. A tal fin, las directrices:

   - estudian el fundamento de la certificación como una herramienta de rendición de cuentas;
   - explican los principales conceptos de las disposiciones sobre certificación recogidas en los artículos 42 y 43; así como
   - explican el ámbito de lo que puede certificarse en virtud de los artículos 42 y 43 y el propósito de la certificación;

[3] Las presentes directrices se referirán a los mecanismos de certificación y a los sellos y marcas de protección de datos conjuntamente como «mecanismos de certificación», véase la sección 1.3.2.
[4] El considerando 100 estipula que debería fomentarse el establecimiento de mecanismos de certificación a fin de aumentar la transparencia y el cumplimiento del presente Reglamento, permitiendo así que los interesados puedan evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.
[5] Véanse las directrices del Grupo de Trabajo del Artículo 29 sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679 (WP253).

- facilitan que el resultado de la certificación sea significativo, inequívoco, tan reproducible como sea posible y comparable con independencia de quién emita la certificación (comparabilidad).

8. El RGPD prevé maneras distintas para que los Estados miembros y las autoridades de control apliquen los artículos 42 y 43. Las directrices ofrecen asesoramiento sobre la interpretación y aplicación de las disposiciones recogidas en los artículos 42 y 43 y ayudarán a los Estados miembros, a las autoridades de control y a los organismos nacionales de acreditación a establecer un planteamiento más coherente y armonizado de la aplicación de mecanismos de certificación de conformidad con el RGPD.

9. El asesoramiento que ofrecen las presentes directrices será pertinente:

   - para las autoridades de control competentes y el Comité Europeo de Protección de Datos (CEPD) a la hora de aprobar criterios de certificación en virtud del artículo 42, apartado 5, del artículo 58, apartado 3, letra f), y del artículo 70, apartado 1, letra o);
   - para los organismos de certificación cuando redacten y revisen los criterios de certificación antes de presentarlos a la autoridad de control competente para su aprobación, tal y como establece el artículo 42, apartado 5;
   - para el CEPD a la hora de aprobar un Sello Europeo de Protección de Datos en virtud del artículo 42, apartado 5, y del artículo 70, apartado 1, letra o);
   - para las autoridades de control cuando elaboren sus propios criterios de certificación;
   - para la Comisión Europea, que está facultada para adoptar actos delegados con el objetivo de especificar las condiciones que deberán tenerse en cuenta en el caso de los mecanismos de certificación con arreglo al artículo 43, apartado 8;
   - para el CEPD a la hora de emitir un dictamen para la Comisión Europea sobre los requisitos de certificación de conformidad con el artículo 70, apartado 1, letra q), y con el artículo 43, apartado 8;
   - para los organismos nacionales de acreditación, que deberán tener en cuenta los criterios de certificación con vistas a acreditar los organismos de certificación de conformidad con la norma EN-ISO/IEC 17065/2012 y los requisitos adicionales con arreglo al artículo 43; así como
   - para los responsables del tratamiento y los encargados del tratamiento a la hora de definir su propia estrategia de cumplimiento del RGPD y de considerar la certificación como un medio para demostrar el cumplimiento.

10. El CEPD publicará directrices aparte para abordar la determinación de criterios para a aprobar mecanismos de certificación como herramientas de transferencia a terceros países u organizaciones internacionales de conformidad con el artículo 42, apartado 2.

1.2 Objetivo de la certificación en virtud del RGPD

11. El artículo 42, apartado 1, dispone que los mecanismos de certificación se establecerán «a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados».

12. El RGPD ilustra el contexto en el que los mecanismos de certificación aprobados pueden utilizarse como un elemento para demostrar el cumplimiento de las obligaciones de los responsables del tratamiento y los encargados del tratamiento con respecto a:

    - la aplicación y demostración de las medidas técnicas y organizativas apropiadas a las que se refieren el artículo 24, apartados 1 y 3, el artículo 25, y el artículo 32, apartados 1 y 3;

    - las garantías suficientes (encargado del tratamiento hacia el responsable del tratamiento) a las que se refieren los apartados 1 y 4 (subencargado hacia encargado del tratamiento) del artículo 28, apartado 5.

13. Dado que la certificación no demuestra el cumplimiento por sí sola, sino que constituye un elemento que puede utilizarse para demostrar dicho cumplimiento, debería emitirse de forma transparente. La demostración del cumplimiento requiere documentación justificativa, especialmente informes por escrito que no solo repitan sino que describan de qué manera se cumplen los criterios y si inicialmente no se cumplían, describan las correcciones y acciones correctivas y su idoneidad, proporcionando así motivos para otorgar y mantener la certificación. Esto incluye el resumen de la decisión concreta por la que se otorga, renueva o retira un certificado. Debería ofrecer los motivos, argumentos y pruebas derivadas de la aplicación de criterios y las conclusiones, dictámenes o inferencias a partir de hechos o premisas recopilados durante la certificación.

1.3 Conceptos clave

14. La siguiente sección examina los conceptos clave recogidos en los artículos 42 y 43. Este análisis amplía la comprensión de los términos básicos y el ámbito de aplicación de la certificación en virtud del RGPD.

1.3.1 Interpretación de «certificación»

15. El RGPD no define el término «certificación». La Organización Internacional de Normalización (ISO) ofrece una definición universal de certificación como un procedimiento mediante el cual «un organismo da garantía por escrito (certificado) de que el producto, servicio o sistema en cuestión cumple unos requisitos específicos». La certificación se entiende también como una «evaluación de la conformidad por una tercera parte» y los organismos de certificación pueden denominarse también «organismos de evaluación de la conformidad» (OEC). En la Norma EN-ISO/IEC 17000:2004 - Evaluación de la conformidad. Vocabulario y principios

generales (a la que se refiere la norma ISO17065), la certificación se define en los siguientes términos: «atestación de un tercero... en relación a productos, procesos y servicios».

16. La atestación es la «emisión de una declaración, con base en una decisión tomada después de la revisión, de que se ha demostrado que se cumplen los requisitos especificados». (Sección 5.2, ISO 17000:2004).

17. En el contexto de la certificación tal y como establecen los artículos 42 y 43 del RGPD, la certificación se referirá a la atestación de un tercero en relación a las operaciones de tratamiento de datos por parte de responsables y encargados del tratamiento.

1.3.2 Mecanismos de certificación, sellos y marcas

18. El RGPD no define los «mecanismos de certificación, sellos o marcas», y utiliza los términos conjuntamente. Un certificado es una declaración de conformidad. Puede utilizarse un sello o marca para indicar la conclusión satisfactoria del procedimiento de certificación. Sello o marca se refiere habitualmente a un logotipo o símbolo cuya presencia (junto con un certificado) indica que el objeto de certificación ha sido valorado de forma independiente en un procedimiento de certificación y es conforme a los requisitos especificados, enunciados en documentos normativos como reglamentos, normas o especificaciones técnicas. Dichos requisitos en el contexto de la certificación con arreglo al RGPD se establecen en los requisitos adicionales que complementan las normas para la acreditación de organismos de certificación en la norma EN-ISO/IEC 17065/2012 y los criterios de certificación aprobados por la autoridad de control competente o por el Comité. Un certificado, sello o marca en virtud del RGPD únicamente puede emitirse tras la evaluación independiente de las pruebas por parte de un organismo acreditado de certificación o autoridad de control competente que indique que los criterios se certificación se han cumplido.

19. La tabla ofrece un ejemplo genérico de un proceso de certificación.

Presentación de una solicitud por parte del responsable o el encargado del tratamiento	**Comprobación formal del organismo de certificación**	**Evaluación Preevaluación**	**Evaluación Evaluación del objetivo de evaluación**	**Evaluación Validación de los resultados**	**Información a las autoridades de control competentes**	**Certificación**	**Seguimiento**	**Renovación de la certificación**
¿La descripción del objetivo de evaluación es inequívoca y completa, incluidas las interfaces?	¿Puede aceptarse la descripción del objetivo de evaluación?	¿Cuáles son los criterios aplicables?	¿Cumple el objetivo de evaluación los criterios?	¿Reflejan el objetivo de evaluación todos los criterios pertinentes especificados?	¿Se han facilitado los motivos para la expedición o retirada de la certificación?	¿Puede otorgarse la certificación?	¿El objetivo de evaluación sigue cumpliendo los criterios?	¿El tratamiento de datos sigue cumpliendo los criterios de certificación?
¿Puede concederse el acceso a las actividades de tratamiento del objetivo de evaluación?	¿Están todos los documentos completos y actualizados?	¿Cuáles son los métodos de evaluación aplicables?	¿Es correcta la documentación del objetivo de evaluación?	¿Se ha documentado suficientemente la evaluación?		¿Están los informes preparados para su publicación?	¿Se utiliza correctamente el certificado/sello/marca?	¿Se han abordado de forma satisfactoria los ámbitos de desarrollo?
artículo 42, apartado 6	artículo 43, apartado 4	artículo 43, apartado 4	artículo 42, apartado 5; artículo 3, apartado 4	artículo 43, apartado 4	artículo 43, apartado 1; artículo 43, apartado 5	artículo 43, apartado 1; artículo 42, apartado 7	artículo 42, apartado 7	artículo 42, apartado 7

2 PAPEL DE LAS AUTORIDADES DE CONTROL

20. El artículo 42, apartado 5, establece que la certificación será expedida por un organismo de certificación acreditado o por una autoridad de control competente. El RGPD no estipula que la expedición de certificaciones sea una función obligatoria de las autoridades de control. En su lugar, el RGPD prevé una serie de modelos distintos. Por ejemplo, una autoridad de control puede elegir una o más de las siguientes opciones:

    - emitir ella misma la certificación de conformidad con su propio sistema de certificación;
    - emitir ella misma la certificación de conformidad con su propio sistema de certificación, pero delegar la totalidad o una parte del proceso de evaluación en terceras partes;
    - crear su propio sistema de certificación y confiar a los organismos de certificación el procedimiento de certificación por el que se emite el certificado; así como
    - alentar al mercado a que desarrolle mecanismos de certificación.

21. Asimismo, una autoridad de control tendrá que considerar su papel a la luz de las decisiones adoptadas a escala nacional con respecto a los mecanismos de acreditación, en particular, si la propia autoridad de control está facultada para acreditar organismos de certificación en virtud del artículo 43, apartado 1, del RGPD. De este modo, cada autoridad de control determinará qué enfoque adopta con el fin de alcanzar el propósito general de la certificación con arreglo al RGPD. Esto se determinará en el contexto no solo de las funciones y los poderes estipulados en los artículos 57 y 58, sino también al considerar la certificación como un factor que hay que tener en cuenta cuando se establezcan multas administrativas, y de manera más general, como un medio de demostrar el cumplimiento.

2.1 La autoridad de control como organismo de certificación

22. En el caso de que una autoridad de control elija realizar la certificación, tendrá que evaluar detenidamente su papel con respecto a las funciones que tiene asignadas con arreglo al RGPD. Su papel en el ejercicio de sus funciones debería ser transparente. Deberá tener en cuenta concretamente la separación de poderes en lo relativo a las investigaciones y las medidas de ejecución con el fin de evitar posibles conflictos de interés.

23. Cuando actúe como organismo de certificación, la autoridad de control deberá garantizar la adecuada puesta en marcha de un mecanismo de certificación y adoptar criterios de certificación o desarrollar los suyos propios. Asimismo, toda autoridad de control que expida certificaciones debe realizar una revisión periódica de dichas certificaciones [artículo 57, apartado 1, letra o)] y tiene poder para retirarlas cuando no se cumplan o dejen de cumplirse los requisitos para la certificación [artículo 58, apartado 2, letra h)]. Con el fin de cumplir dichos requisitos, es de utilidad establecer un procedimiento de certificación y condiciones relativas al proceso, y si no se estipula de otra manera, p. ej. mediante una ley nacional, establecer un acuerdo legalmente exigible para la prestación de actividades de certificación con cada organización solicitante. Debería garantizarse que este acuerdo de certificación

requiera que el solicitante cumpla al menos con los criterios de certificación, incluidas las disposiciones necesarias para realizar la evaluación, supervisar el cumplimiento de los criterios y realizar una revisión periódica que incluya el acceso a información o a instalaciones, documentación y publicación de informes y resultados e investigación de reclamaciones. Además, se espera que la autoridad de control se ajuste a los requisitos recogidos en las directrices para acreditación de organismos de certificación además de a los requisitos contemplados en el artículo 43, apartado 2.

2.2 Tareas ulteriores de la autoridad de control con respecto a la certificación

24. En los Estados miembros en los que los organismos de certificación están activos, la autoridad de control tiene poder y funciones, independientemente de sus propias actividades para:

    - evaluar los criterios de un sistema de certificación y elaborar un proyecto de decisión (artículo 42, apartado 5);
    - comunicar al Comité el proyecto de decisión cuando pretenda aprobar los criterios de certificación [artículo 64, apartado 1, letra c); artículo 64, apartado 7] y considerar el dictamen del Comité [artículo 64, apartado 1, letra c), y artículo 70, apartado 1, letra t)];
    - aprobar los criterios de certificación [artículo 58, apartado 3, letra f)] antes de que pueda tener lugar la acreditación y la certificación [artículo 42, apartado 5, y artículo 43, apartado 2, letra b)];
    - publicar los criterios de certificación (artículo 43, apartado 6);
    - actuar como autoridad competente en sistemas de certificación a escala de la UE que pudieran dar lugar a Sellos Europeos de Protección de Datos [artículo 42, apartado 5, y artículo 70, apartado 1, letra o)]; así como
    - ordenar a un organismo de certificación a) que no emita una certificación o b) que retire una certificación cuando los requisitos para la certificación (procedimientos o criterios de certificación) no se cumplan o dejen de cumplirse [artículo 58, apartado 2, letra h)].

25. El RGPD impone a la autoridad de control la tarea de aprobar los criterios de certificación pero no la de elaborar los criterios. Con el fin de aprobar los criterios de certificación en virtud del artículo 42, apartado 5, una autoridad de control debería contar con un conocimiento claro de qué se puede esperar, concretamente en lo relativo al alcance y contenido para demostrar el cumplimiento de RGPD y con respecto a su labor de controlar y hacer que se aplique el reglamento. El anexo proporciona orientación para garantizar un enfoque armonizado a la hora de evaluar los criterios con el propósito de aprobarlos.

26. El artículo 43, apartado 1, exige a los organismos de certificación que informen a su autoridad de control antes de emitir o renovar certificaciones, a fin de que la autoridad de control competente pueda ejercer sus poderes correctivos en virtud del artículo 58, apartado 2, letra h). Además, el artículo 43, apartado 5, exige también a los organismos de certificación

que comuniquen a la autoridad de control competente las razones de la expedición o retirada de la certificación solicitada. Aunque el GDPR permite a las autoridades de control determinar cómo recibir, confirmar, revisar y tratar esta información de manera operativa (por ejemplo, esto podría incluir soluciones tecnológicas que permitan a los organismos de certificación presentar informes), debe establecerse un proceso y criterios para tratar la información y los informes facilitados en cada proyecto de certificación satisfactorio por parte del organismo de certificación de conformidad con el artículo 43, apartado 1. Sobre la base de esta información, la autoridad de control puede ejercer su poder para ordenar al organismo de certificación que retire o no otorgue una certificación [artículo 58, apartado 2, letra h)] y que supervise y haga que se apliquen los requisitos y criterios de la certificación en virtud del RGPD [artículo 57, apartado 1, letra a), y artículo 58, apartado 2, letra h)]. Ello contribuirá a lograr un enfoque armonizado y la comparabilidad de la certificación por distintos organismos de certificación y a que las autoridades de control tengan información sobre el estado de certificación de un organismo.

3 PAPEL DE UN ORGANISMO DE CERTIFICACIÓN

27. El papel de un organismo de certificación es emitir, revisar, renovar y retirar certificaciones (artículo 42, apartados 5 y 7) sobre la base de un mecanismo de certificación y criterios aprobados (artículo 43, apartado 1). Esto requiere que el organismo de certificación o el propietario de un sistema de certificación determine y establezca criterios de certificación y procedimientos de certificación, entre ellos, procedimientos para supervisar el cumplimiento, la revisión, la tramitación de reclamaciones y la retirada. Los criterios de certificación se revisan como parte del proceso de acreditación, que tiene en cuenta las normas y procedimientos en virtud de los cuales se emiten certificados, sellos o marcas [artículo 43, apartado 2, letra c)].

28. La existencia de un mecanismo de certificación y de criterios de certificación es necesaria para que el organismo de certificación obtenga acreditación en virtud del artículo 43. Uno de los efectos más importantes de la labor de un organismo de certificación se deriva del ámbito de aplicación y el tipo de criterios de certificación, lo cual repercute en los procedimientos de certificación y viceversa. Algunos criterios pueden, por ejemplo, requerir métodos específicos de evaluación como inspecciones *in situ* y revisión de códigos. Dichos procedimientos son obligatorios para la acreditación y se explican con mayor detalle en las directrices sobre acreditación.

29. El RGPD exige al organismo de certificación que facilite a las autoridades de control la información, en particular sobre certificaciones individuales, que sea necesaria para supervisar la aplicación del mecanismo de certificación [artículo 42, apartado 7; artículo 43, apartado 5; artículo 58, apartado 2, letra h)].

4 APROBACIÓN DE LOS CRITERIOS DE CERTIFICACIÓN

30. Los criterios de certificación son parte integrante de cualquier mecanismo de certificación. Por consiguiente, el RGPD requiere que la autoridad de control competente apruebe los criterios de certificación de un mecanismo de certificación [artículo 42, apartado 5, y artículo 43,

apartado 2, letra b)]. En el caso de un Sello Europeo de Protección de Datos, será el CEPD quien deba aprobar los criterios de certificación [artículo 42, apartado 5, y artículo 70, apartado 1, letra o)]. Ambas vías para la aprobación de criterios de certificación se explican más adelante.

31. El CEPD reconoce los siguientes fines para la aprobación de criterios de certificación:

    - reflejar correctamente los requisitos y principios relativos a la protección de las personas físicas en lo que respecta al tratamiento de datos personales recogidos en el Reglamento (UE) 2016/679; así como
    - contribuir a la aplicación coherente del RGPD.

32. La aprobación se otorga sobre la base de que el requisito del RGPD de que el mecanismo de certificación permita a los responsables y encargados del tratamiento de datos demostrar el cumplimiento del RGPD se refleje plenamente en los criterios de certificación.

4.1 Aprobación de los criterios por la autoridad de control competente

33. Los criterios de certificación deben ser aprobados por la autoridad de control competente antes o durante el proceso de acreditación de un organismo de certificación. La aprobación se requiere también para sistemas o conjuntos de criterios actualizados o adicionales en virtud de la norma ISO 17065 por el mismo organismo de certificación, antes de su uso de los mecanismos de certificación modificados [artículo 42, apartado 5, y artículo 43, apartado 2, letra b)]. Las autoridades de control tratarán todas las solicitudes de aprobación de criterios de certificación de forma justa y no discriminatoria, de acuerdo con un procedimiento de acceso público que especifique las condiciones generales que deben cumplirse y la descripción del proceso de aprobación.

34. Un organismo de certificación solo puede emitir una certificación en un Estado miembro concreto de acuerdo con los criterios aprobados por la autoridad de control de dicho Estado miembro. En otras palabras, los criterios de certificación deben ser aprobados por la autoridad de control competente allí donde el organismo de certificación tenga la intención de ofrecer certificación y obtenga la acreditación. Para información sobre sistemas de certificación a escala europea, véase la sección que figura a continuación.

4.2 Aprobación de criterios por parte del CEPD para el Sello Europeo de Protección de Datos

35. Un organismo de certificación puede también emitir una certificación de acuerdo a criterios aprobados por el CEPD para la emisión de un Sello Europeo de Protección de Datos. Los criterios de certificación aprobados por el CEPD con arreglo al artículo 63 pueden dar lugar a un Sello Europeo de Protección de Datos (artículo 42, apartado 5). A la luz de los convenios existentes en materia de certificación y acreditación, el CEPD reconoce que es conveniente evitar la fragmentación del mercado de la certificación de la protección de datos. Señala que el artículo 42, apartado 1, establece que los Estados miembros, las autoridades de control, el

Comité y la Comisión promoverán la creación de mecanismos de certificación, en particular a escala de la Unión.

4.2.1 Solicitud de aprobación

36. La solicitud de aprobación de los criterios con arreglo al artículo 42, apartado 5, y al artículo 70, apartado 1, letra o), por parte del CEPD debe presentarse a través de una autoridad de control competente y debería indicar la intención del propietario del sistema, el candidato o el organismo de certificación acreditado de ofrecer los criterios en un mecanismo de certificación dirigido a responsables y encargados del tratamiento en todos los Estados miembros. La autoridad de control competente facilitará al CEPD un proyecto cuando considere que los criterios podrían ser aprobados por dicho Comité.

37. La elección del lugar en el que se presenta una solicitud para la aprobación de criterios se basará en dónde se encuentre la sede de los propietarios del sistema de certificación o de los organismos de certificación.

38. Si un organismo de certificación presenta una solicitud, normalmente lo hará en el proceso de solicitud de acreditación o una vez acreditado por la autoridad de control competente o por el organismo nacional de acreditación de su Estado miembro. El hecho de que el organismo de certificación ya haya sido acreditado para un mecanismo de certificación del RGPD puede simplificar el proceso de aprobación.

4.2.2 Criterios relativos al Sello Europeo de Protección de Datos

39. El CEPD coordinará el proceso de evaluación y aprobará los criterios para un Sello Europeo de Protección de Datos según se requiera. La evaluación abordará aspectos tales como: el ámbito de aplicación de los criterios y la capacidad para funcionar como una certificación común. Cuando los criterios sean aprobados por el CEPD, se espera que la autoridad de control competente correspondiente a la sede en la UE del organismo de certificación tramite las reclamaciones sobre el propio mecanismo e informe a otras autoridades de control. Dicha autoridad de control tendrá también competencia para adoptar medidas contra el organismo de certificación. Según corresponda, la autoridad de control competente informará al resto de autoridades de control y al CEPD.

40. Los criterios de certificación relativos a una certificación común están sujetos a las necesidades de toda la UE y deben proporcionar un mecanismo específico para tratar dichas necesidades. Los mecanismos de certificación europeos deben estar previstos para su uso en todos los Estados miembros. En virtud del artículo 42, apartado 5, el mecanismo relativo a un Sello Europeo de Protección de Datos, así como sus criterios deben ser personalizables de manera que tengan en cuenta las normativas nacionales específicas del sector cuando proceda, por ejemplo, para el tratamiento de datos en centros escolares, y deben prever su aplicación en toda la UE.

41. Ejemplo: Una escuela internacional que ofrece enseñanza a interesados en la Unión está establecida en un Estado miembro «A». La escuela desea certificar su proceso de solicitud en

línea con un sistema de certificación a escala de la UE con el fin de obtener el Sello Europeo de Protección de Datos. Esta escuela pretende solicitar la certificación de las operaciones de tratamiento de datos ofrecida por un organismo de certificación establecido en el Estado miembro «B» sobre la base del Sello Europeo de Protección de Datos. Los criterios del Sello diseñados y documentados en el correspondiente mecanismo deben permitir tener en cuenta la normativa sobre centros de enseñanza aplicable en el Estado miembro «A». Los criterios deberían también requerir que el proceso de solicitud en línea de la escuela proporcione información y tenga en cuenta los requisitos aplicables en materia de protección de datos en el Estado miembro, que pueden diferir en otros Estados miembros. Un ejemplo serían los conjuntos de datos personales que deben enviarse para la solicitud, p.ej., calificaciones de la escuela infantil o resultados de pruebas, distintos periodos de conservación, recogida o tratamiento de datos financieros o biométricos, otras limitaciones en el tratamiento de datos.

- Los criterios de alto nivel para la aprobación de un mecanismo relativo a un Sello Europeo de Protección de Datos incluyen:
  - criterios aprobados por el Comité;
  - solicitud en distintas jurisdicciones que refleje, cuando sea preciso, los requisitos jurídicos nacionales y la normativa específica del sector;
  -
- criterios armonizados que puedan personalizarse para reflejar los requisitos nacionales;
  - descripción del mecanismo de certificación, especificando:
  - los acuerdos de certificación que reconozcan requisitos paneuropeos;
  - procedimientos para garantizar y ofrecer soluciones a las variaciones nacionales y garantizar que el Sello contribuye a demostrar el cumplimiento del RGPD; así como
  - el idioma de los informes dirigidos a todas las autoridades de control afectadas.

42. El anexo contiene orientaciones sobre los criterios del Sello Europeo de Protección de Datos.

4.2.3 Papel de la acreditación

43. Tal y como se ha señalado en la sección 4.2.1, cuando se determina que los criterios son adecuados para una certificación común y han sido aprobados como tales por el Comité, de conformidad con el artículo 42, apartado 5, pueden acreditarse los organismos de certificación para realizar la certificación a escala de la UE en virtud de dichos criterios.

44. Los sistemas que están previstos únicamente para ofertarse en determinados Estados miembros no serán idóneos para la obtención de los Sellos de la UE. La acreditación para el ámbito de aplicación de un Sello Europeo de Protección de Datos requerirá acreditación en el Estado miembro en el que se encuentre la sede del organismo de certificación que tiene la intención de gestionar el sistema, es decir, el organismo responsable de emitir las

certificaciones y gestionar las actividades de certificación de sus entidades y filiales en otros Estados miembros. En los casos en los que otros establecimientos u oficinas gestionen y realicen certificaciones de forma autónoma, cada uno de dichos establecimientos u oficinas deberá contar con acreditación individual en el Estado miembro en el que esté establecido. En otras palabras, la acreditación es necesaria solo en el Estado miembro de la sede del organismo de certificación cuando únicamente dicha sede emita los certificados. Por el contrario, cuando otros establecimientos del organismo de certificación emitan también certificados, dichos establecimientos deberán asimismo estar acreditados.

45. En consecuencia, si un organismo de certificación no ha sido acreditado para certificar con arreglo al Sello Europeo de Protección de Datos, no pueden utilizarse los criterios aprobados por el CEPD y no puede ofrecerse el Sello.

5 ELABORACIÓN DE LOS CRITERIOS DE CERTIFICACIÓN

46. El RGPD estableció el marco para la elaboración de los criterios de certificación. Si bien los requisitos fundamentales relativos al procedimiento de certificación se abordan en los artículos 42 y 43 ofreciendo, a su vez, criterios esenciales para los procedimientos de certificación, la base de los criterios de certificación debe derivarse de los principios y normas del RGPD y debe contribuir a proporcionar garantías de que estos se cumplen.

47. La elaboración de criterios de certificación debería centrarse en la verificabilidad, relevancia e idoneidad de los criterios de certificación para demostrar el cumplimiento del Reglamento. Los criterios de certificación deben formularse de manera que sean claros y comprensibles y que permitan su aplicación práctica.

48. Cuando se redacten criterios de certificación se tendrán en cuenta, entre otros, los siguientes aspectos de cumplimiento para respaldar la evaluación de la operación de tratamiento de datos, según corresponda:

- la licitud del tratamiento con arreglo al artículo 6;
- los principios del tratamiento de datos de conformidad con el artículo 5;
- los derechos de los interesados a tenor de los artículos 12 a 23;
- la obligación de notificar violaciones de la seguridad de los datos de conformidad con el artículo 33;
- la obligación de proteger los datos desde el diseño y por defecto en virtud del artículo 25;
- si se ha realizado una evaluación de impacto con arreglo al artículo 35, apartado 7, letra d), cuando proceda; así como
- las medidas técnicas y organizativas adoptadas en virtud del artículo 32.

49. La medida en la que dichas consideraciones se reflejen en los criterios podrá variar dependiendo del ámbito de aplicación de la certificación que puede incluir el tipo de operación u operaciones de tratamiento y la esfera (p.ej., el sector sanitario) de la certificación.

5.1 Qué puede certificarse en el marco del RGPD

50. El CEPD considera que el RGPD proporciona un gran margen para lo que puede certificarse con arreglo a dicho Reglamento, siempre que se haga hincapié en contribuir a demostrar el cumplimiento de este Reglamento en las operaciones de tratamiento de los responsables y los encargados del tratamiento (artículo 42, apartado 1).

51. A la hora de evaluar una operación de tratamiento, deben tenerse en cuenta, cuando sea pertinente, los siguientes tres componentes fundamentales:

    1. datos personales (ámbito de aplicación material del RGPD);
    2. sistemas técnicos: la infraestructura, como los equipos y programas informáticos utilizados para el tratamiento de los datos personales; así como
    3. los procesos y procedimientos relacionados con la operación u operaciones de tratamiento.

52. Cada componente utilizado en las operaciones de tratamiento debe ser evaluado con respecto a los criterios establecidos. Pueden influir al menos cuatro factores importantes: 1) la organización y la estructura jurídica del responsable o del encargado del tratamiento; 2) el departamento, el entorno y las personas que participan en la operación u operaciones de tratamiento; 3) la descripción técnica de los elementos que deben evaluarse; y finalmente 4) la infraestructura de TI que respalda la operación de tratamiento, incluidos los sistemas operativos, los sistemas virtuales, las bases de datos, los sistemas de autenticación y autorización, los encaminadores y cortafuegos, los sistemas de almacenamiento, la infraestructura de comunicación o el acceso a internet y otras medidas técnicas conexas.

53. Los tres componentes son pertinentes para el diseño de procedimientos y criterios de certificación. Dependiendo del objeto de certificación, puede variar la medida en que se tiene en cuenta cada uno de ellos. Por ejemplo, en algunos casos, algunos componentes pueden ser descartados si se considera que no son relevantes para el objeto de la certificación.

54. Con el fin de especificar con más detalle qué puede certificarse con arreglo al RGPD, el Reglamento contiene más orientación. Del artículo 42, apartado 7, se deduce que las certificaciones a tenor del RGPD únicamente se conceden a los responsables del tratamiento de datos y a los encargados del tratamiento de datos, lo que excluye, por ejemplo, la certificación de los delegados del tratamiento de datos. El artículo 43, apartado 1, letra b), se refiere a la norma ISO 17065 que prevé la acreditación de organismos de certificación que evalúan la conformidad de productos, servicios y procesos. Una operación de tratamiento o un conjunto de operaciones puede dar lugar a un producto o servicio según la terminología de la ISO/17065 y, como tal, puede ser objeto de certificación. Por ejemplo, el tratamiento de datos de empleados para el pago del salario o la gestión de permisos es un conjunto de

operaciones en el sentido del RGPD y puede dar lugar a un producto, proceso o servicio según la terminología de ISO.

55. A la luz de estas reflexiones, el CEPD considera que el ámbito de aplicación de la certificación con arreglo al RGPD va dirigido a operaciones de tratamiento o conjuntos de operaciones de tratamiento. Dichas operaciones pueden incluir procesos de gobernanza en el sentido de medidas organizativas, es decir, como partes integrantes de una operación de tratamiento (p.ej., los procesos de gobernanza establecidos para la tramitación de reclamaciones como parte del tratamiento de datos de empleados para el pago del salario).

56. Con el fin de evaluar la conformidad de las operaciones de tratamiento de datos con los criterios de certificación debe proporcionarse un caso práctico. Por ejemplo, el cumplimiento del uso de una infraestructura técnica desplegada en una operación de tratamiento de datos depende de las categorías de datos que está diseñada para procesar. Las medidas organizativas dependen de las categorías y la cantidad de datos y de la infraestructura técnica utilizada para el tratamiento, teniendo en cuenta la naturaleza, ámbito de aplicación, contenido y fines del tratamiento, así como los riesgos que plantea para los derechos y libertades de los interesados.

57. Asimismo, debe tenerse en cuenta que las aplicaciones informáticas pueden diferir ampliamente aunque sirvan para los mismos fines de tratamiento. Por lo tanto, a la hora de definir el ámbito de aplicación de los mecanismos de certificación y de elaborar los criterios de certificación debe tenerse presente este aspecto, es decir, el ámbito de aplicación de la certificación, y los criterios no deben ser tan limitados que excluyan aplicaciones informáticas diseñadas de modo distinto.

5.2 Determinar el objeto de certificación

58. El ámbito de aplicación de un mecanismo de certificación debe distinguirse del objeto –también denominado el objetivo de evaluación– en proyectos de certificación individuales en el marco de un mecanismo de certificación. Un mecanismo de certificación puede definir su ámbito de aplicación de manera general o en relación a un tipo o ámbito específico de operaciones de tratamiento de datos y, de este modo, puede ya identificar los objetos de certificación que se incluyen en el ámbito de aplicación del mecanismo de certificación (p.ej., almacenamiento seguro y protección de datos personales contenidos en una bóveda digital). En cualquier caso, únicamente puede tener lugar una evaluación fiable y significativa de la conformidad si el objeto concreto de un proyecto de certificación se describe con precisión. Debe describirse con claridad qué operaciones de tratamiento de datos se incluyen en el objeto de certificación y posteriormente en los componentes fundamentales, es decir, qué datos, procesos e infraestructura técnica se evaluarán y cuáles no. Al hacer esto, deben asimismo tenerse en cuenta siempre las interconexiones con otros procesos. Es evidente que lo que no se conoce no puede formar parte de la evaluación y, por tanto, no puede certificarse. En cualquier caso, el objeto individual de certificación debe ser significativo con respecto al mensaje o afirmación efectuada en o por la certificación y no debería inducir a error al usuario, cliente o consumidor.

59. [Ejemplo 1]

Un banco ofrece a sus clientes un sitio web para operaciones bancarias por internet. En el marco de este servicio, existe la posibilidad de realizar transferencias, comprar acciones, iniciar órdenes de pago permanentes y gestionar la cuenta. El banco desea certificar lo siguiente en el marco de un mecanismo de certificación de protección de datos con un ámbito de aplicación general basado en criterios genéricos:

a) Inicio de sesión seguro

El inicio de sesión seguro es una operación de tratamiento de datos comprensible para el usuario final y pertinente desde una perspectiva de protección de datos, puesto que desempeña un papel importante a la hora de garantizar la seguridad de los datos personales en cuestión. Por lo tanto, esta operación de tratamiento es necesaria para un inicio de sesión seguro y puede, así, constituir un objetivo de evaluación significativo si el certificado indica claramente que solo se certifica la operación de tratamiento del inicio de sesión.

b) Interfaz de usuario de la web

Si bien la interfaz de usuario de la web puede ser pertinente desde una perspectiva de protección de datos, no es comprensible para el usuario final y, por tanto, no puede ser un objetivo de evaluación significativo. Además, no queda claro para el usuario qué servicios del sitio web y, por tanto, qué operaciones de tratamiento de datos están cubiertos por la certificación.

c) Banca por internet

La interfaz de usuario de la web junto con el «back-end» (parte del servidor) son operaciones de tratamiento proporcionadas dentro del servicio de banca por internet que pueden tener sentido para el usuario. En este contexto, ambos deben incluirse en el objetivo de evaluación, mientras que las operaciones de tratamiento de datos que no tienen una relación directa con la prestación del servicio de banca por internet, como operaciones de tratamiento destinadas a prevenir el blanqueo de capitales, pueden excluirse del objeto de evaluación.

No obstante, los servicios de banca por internet ofrecidos por el banco a través de su sitio web pueden incluir también otros servicios que, a su vez, requieran sus propias operaciones de tratamiento de datos. En este contexto, otros servicios podrían ser, por ejemplo, la oferta de un producto de seguros. Dado que este servicio adicional no está directamente ligado al propósito de prestar servicios de banca por internet, puede excluirse del objetivo de evaluación. Si este servicio adicional (seguro) se excluye del objetivo de evaluación, las interfaces de dicho servicio integradas en el sitio web son parte del objetivo de evaluación y deben, por tanto, describirse con el fin de distinguir claramente los servicios. Dicha descripción es necesaria para identificar y evaluar posibles flujos de datos entre los dos servicios.

60. [Ejemplo 2]

Un banco ofrece a sus clientes un servicio que les permite combinar la información relacionada con distintas cuentas y tarjetas de crédito de varios bancos (agregación de cuentas). El banco desea certificar dicho servicio en virtud del RGPD. La autoridad de control competente ha aprobado un conjunto específico de criterios de certificación centrados en este tipo de actividad. El ámbito de aplicación del mecanismo de certificación únicamente aborda los siguientes aspectos de cumplimiento:

- autenticación del usuario; así como
- formas aceptables de obtener los datos que van a agregarse de otros bancos o servicios.

Dado que el ámbito de aplicación de este mecanismo de certificación define el objetivo de evaluación por sí mismo, no es posible acotar con sentido el objetivo de evaluación dentro del ámbito propuesto y certificar únicamente determinadas características o una única actividad de tratamiento de datos. En estas circunstancias, un objetivo de evaluación debe ser igual a un ámbito de aplicación específico.

5.3 Métodos de evaluación y metodología de valoración

61. Una valoración de la conformidad para contribuir a demostrar el cumplimiento de las operaciones de tratamiento de datos requiere identificar y determinar los métodos de evaluación y la metodología de valoración. Es importante saber si la información para la valoración se recopila solo a partir de documentación (lo cual no sería en sí mismo suficiente) o si se recopila activamente *in situ* y mediante acceso directo o indirecto. El modo en el que la información se recoge tiene consecuencias en cuanto a la relevancia de la certificación y, por tanto, debería definirse y describirse.

    Los procedimientos destinados a la emisión y revisión periódica de certificaciones deberían incluir especificaciones para identificar el nivel apropiado de evaluación (detalle y granularidad) con el fin de cumplir los criterios de certificación y deberían incluir el suministro de:

    - información y especificación de los métodos de valoración aplicados y de las conclusiones obtenidas, p.ej., durante auditorías *in situ* o a partir de documentación,
    - métodos de evaluación que se centren en las operaciones de tratamiento (datos, sistemas, procesos) y el fin del tratamiento,
    - identificación de las categorías de datos, las necesidades de protección y si participan los encargados del tratamiento de datos o terceras partes,
    - identificación de las funciones y existencia de un mecanismo de control de acceso definido en torno a las funciones y responsabilidades.

62. El detalle con el que se realiza la evaluación repercute en la relevancia y el valor de la certificación. Al reducir la profundidad de la evaluación por razones pragmáticas o para reducir costes, la relevancia de una certificación de protección de datos se verá mermada. Por otra

parte, las decisiones sobre la granularidad de la evaluación pueden exceder las capacidades financieras del solicitante y, con frecuencia, también la capacidad de los evaluadores y auditores. A fin de demostrar el cumplimiento puede que no siempre sea esencial llegar a un análisis muy detallado de los sistemas informáticos utilizados para seguir manteniendo el sentido.

5.4 Documentación de la valoración

63. La documentación de la certificación debería ser exhaustiva y completa. La falta de documentación supone que no pueda llevarse a cabo una correcta valoración. La función esencial de la documentación de la certificación es que aporta transparencia en el proceso de evaluación en el marco del mecanismo de certificación. La documentación da respuesta a las cuestiones relativas a los requisitos establecidos por la ley. Los mecanismos de certificación deberían contemplar una metodología de documentación normalizada. A partir de ahí, la evaluación permitiría comparar la documentación de certificación con la situación real *in situ* y con respecto a los criterios de certificación.

64. Una documentación exhaustiva sobre lo que se ha certificado y sobre la metodología usada contribuye a la transparencia. Con arreglo al artículo 43, apartado 2, letra c), los mecanismos de certificación deberían establecer procedimientos que permitieran la revisión de las certificaciones. Con el fin de posibilitar que la autoridad de control evalúe si la certificación puede reconocerse en investigaciones oficiales y en qué medida, el método más apropiado de comunicación puede ser aportar documentación detallada. La documentación elaborada durante la evaluación debería, por tanto, centrarse en tres aspectos principales:

    - consonancia y coherencia de los métodos de evaluación aplicados;
    - métodos de evaluación dirigidos a demostrar que el objeto de certificación cumple los criterios de certificación y, por tanto, el Reglamento; así como
    - que los resultados de la evaluación hayan sido validados por un organismo de certificación independiente e imparcial.

5.5 Documentación de los resultados

65. El considerando 100 proporciona información sobre los objetivos que se persiguen con la introducción de la certificación.

«A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes».

66. La documentación y la comunicación de los resultados desempeñan un papel importante a la hora mejorar la transparencia. Los organismos de certificación que utilizan mecanismos de certificación, sellos o marcas dirigidos a los interesados (en su papel de consumidores o clientes) deberían proporcionar información fácilmente disponible, inteligible y significativa

sobre la operación u operaciones de tratamiento de datos certificadas. Esta información pública debería incluir como mínimo:

- la descripción del objetivo de evaluación;
- la referencia a los criterios aprobados aplicados al objetivo de evaluación específico;
- la metodología utilizada en la evaluación de los criterios (evaluación *in situ*, documentación, etc.); así como
- la duración de la validez del certificado; así como
- debería permitir a las autoridades de control y al público la comparación de los resultados.

6 GUÍA PARA LA DEFINICIÓN DE LOS CRITERIOS DE CERTIFICACIÓN

67. Los criterios de certificación son parte integrante de un mecanismo de certificación. El procedimiento de certificación incluye los requisitos relativos a cómo, por quién, en qué medida y la granularidad con la que se realizará la evaluación que tendrá lugar en proyectos concretos de certificación sobre un objeto específico u objetivo de evaluación. Los criterios de certificación proporcionan los requisitos nominales con respecto a los cuales se valora la operación de tratamiento de datos real definida en el objetivo de evaluación. Las presentes directrices para la definición de los criterios de certificación proporcionan asesoramiento general que facilitará la valoración de los criterios de certificación a efectos de su aprobación.
    - Las siguientes consideraciones generales deben tenerse en cuenta a la hora de aprobar o definir criterios de certificación. Los criterios de certificación deben:
    - ser uniformes y verificables,
    - ser auditables con el fin de facilitar la evaluación de operaciones de tratamiento de datos en virtud del RGPD, especificando, en particular, los objetivos y la guía de aplicación para lograr dichos objetivos;
    - ser pertinente con respecto al público objetivo (p.ej., entre empresas y empresas hacia clientes);
    - tener en cuenta otras normas (tales como las normas ISO, normas a escala nacional) y, cuando proceda, ser interoperables con ellas; así como
    - ser flexibles y ampliables para su aplicación a distintos tipos y tamaños de organizaciones, entre ellas, microempresas, y pequeñas y medianas empresas de conformidad con el artículo 42, apartado 1, y el enfoque basado en el riesgo con arreglo al considerando 77.
68. Una pequeña empresa local, por ejemplo, un minorista, normalmente lleva a cabo operaciones de tratamiento de datos menos complejas que una gran empresa minorista multinacional. Si bien los requisitos relativos a la licitud de las operaciones de tratamiento de datos son los

mismos, debe tenerse en cuenta el alcance del tratamiento y su complejidad; de ello se deduce que es preciso que los mecanismos de certificación y sus criterios sean ampliables en función de la actividad de tratamiento de datos en cuestión.

6.1 Normas existentes

69. Los organismos de certificación deberán considerar de qué manera los criterios específicos tienen en cuenta instrumentos pertinentes ya existentes, tales como códigos de conducta, normas técnicas o iniciativas reglamentarias y jurídicas nacionales. Lo ideal sería que los criterios fueran interoperables con normas existentes que puedan ayudar al responsable del tratamiento y al encargado del tratamiento a cumplir sus obligaciones en virtud del RGPD. No obstante, si bien las normas de la industria se centran en la protección y seguridad de la organización frente a amenazas, el RGPD va dirigido a proteger los derechos fundamentales de las personas físicas. Esta distinta perspectiva debe tenerse en cuenta a la hora de diseñar criterios o de aprobar criterios o mecanismos de certificación basados en normas industriales.

6.2 Definición de criterios

70. Los criterios de certificación deben corresponderse con la declaración de certificación (mensaje o afirmación) de un mecanismo o sistema de certificación y adecuarse a las expectativas que genera. El nombre de un mecanismo de certificación puede ya identificar el ámbito de aplicación y tendrá consecuencias para el establecimiento de los criterios.

71. [Ejemplo 3]

    Un mecanismo denominado «HealthPrivacyMark» (marca de privacidad de salud) debería limitar su ámbito de aplicación al sector sanitario. El nombre del sello genera la expectativa de que se han examinado los requisitos de protección de datos en relación con los datos relativos a la salud. Por consiguiente, los criterios de este mecanismo deben ser adecuados para valorar los requisitos de protección de datos en dicho sector.

72. [Ejemplo 4]

    Un mecanismo que tenga que ver con la certificación de operaciones de tratamiento de datos que comprendan sistemas de gobernanza en el tratamiento de datos debería identificar criterios que permitan el reconocimiento y evaluación de procesos de gobernanza y sus medidas técnicas y organizativas complementarias.

73. [Ejemplo 5]

    Los criterios de un mecanismo relacionado con necesidades de computación en la nube deben tener en cuenta los requisitos técnicos especiales necesarios para el uso de servicios basados en la nube. Por ejemplo, si los servidores están fuera de la UE, los criterios deben considerar las condiciones establecidas en el capítulo V del RGPD con respecto a las transferencias de datos a terceros países.

74. Los criterios diseñados para ajustarse a distintos objetivos de evaluación en distintos sectores o Estados miembros deberían: permitir la aplicación a circunstancias distintas; permitir la determinación de medidas adecuadas para ajustarse a operaciones de tratamiento de datos pequeñas, medianas o grandes y reflejar los riesgos de diversa gravedad y probabilidad para los derechos y libertades de las personas físicas, en consonancia con el RGPD. Por consiguiente, los procedimientos de certificación (p.ej., para la documentación, prueba o método y detalle de la evaluación) que complementan los criterios deben responder a dichas necesidades y permitir y contar con normas, por ejemplo, para aplicar los criterios pertinentes en proyectos individuales de certificación. Los criterios deben aportar una valoración sobre si se han proporcionado garantías suficientes para la aplicación de medidas técnicas y organizativas adecuadas.

6.3 Duración de los criterios de certificación

75. Aunque los criterios de certificación deben ser fiables a lo largo del tiempo, no deberían ser inmutables. Estarán sujetos a revisión, por ejemplo, cuando:

- se modifique el marco jurídico;
- los términos y disposiciones sean objeto de interpretación por sentencias del Tribunal de Justicia de la Unión Europea; o
- haya evolucionado el estado de la técnica.

Por el Comité Europeo de Protección de Datos

El Presidente

(Andrea Jelinek)

ANEXO 1: FUNCIONES Y PODERES DE LAS AUTORIDADES DE CONTROL EN RELACIÓN A LA CERTIFICACIÓN DE CONFORMIDAD CON EL RGPD

	Disposiciones	Requisitos
Tareas	Artículo 43, apartado 6	Requiere que la autoridad de control haga públicos los criterios a los que se refiere el artículo 42, apartado 5, de forma fácilmente accesible y los transmita al Comité.
	Artículo 57, apartado 1, letra n)	Exige a la autoridad de control que apruebe los criterios de certificación con arreglo al artículo 42, apartado 5.
	Artículo 57, apartado 1, letra o)	Establece que, si procede (es decir, cuando expida una certificación), la autoridad de control deberá llevar a cabo una revisión periódica de las certificaciones expedidas de conformidad con el artículo 42, apartado 7.
	Artículo 64, apartado 1, letra c)	Requiere que la autoridad de control comunique su proyecto de decisión al Comité, cuando prevea aprobar los criterios de certificación a los que se refiere el artículo 42, apartado 5.
Poderes	Artículo 58, apartado 1, letra c)	Establece que la autoridad de control tendrá poder para llevar a cabo revisiones de las certificaciones en virtud del artículo 42, apartado 7;
	Artículo 58, apartado 2, letra h)	Dispone que la autoridad de control tiene poder para retirar una certificación u ordenar al organismo de certificación que retire una certificación u ordenar al organismo de certificación que no se emita una certificación.
	Artículo 58, apartado 3, letra e)	Establece que la autoridad de control tiene poder para acreditar los organismos de certificación.
	Artículo 58, apartado 3, letra f)	Estipula que la autoridad de control tiene poder para expedir certificaciones y aprobar criterios de certificación.
	Artículo 58, apartado 3, letra e)	Dispone que la autoridad de control tiene poder para acreditar organismos de certificación.
	Artículo 58, apartado 3, letra f)	Estipula que la autoridad de control tiene poder para expedir certificaciones y aprobar criterios de certificación.

ANEXO 2

1 INTRODUCCIÓN

El anexo 2 ofrece una guía para la revisión y la evaluación de los criterios de certificación con arreglo al artículo 42, apartado 5. En él se identifican los temas que la autoridad de control en materia de protección de datos y el CEPD considerarán y aplicarán a los efectos de aprobar los criterios de certificación de un mecanismo de certificación. Los organismos de certificación y los propietarios de sistemas que deseen redactar y presentar criterios para su aprobación deberán considerar las preguntas. La lista no es exhaustiva, pero presenta los temas mínimos que deben considerarse. No todas las preguntas serán pertinentes; sin embargo, deberán considerarse cuando se redacten los criterios y sea necesario un razonamiento para explicar por qué los criterios no tratan aspectos específicos. Algunas preguntas se repiten, ya que se han redactado desde diferentes puntos de vista. Esta guía debe considerarse de acuerdo con las disposiciones legales previstas en el RGPD y, en su caso, en la legislación nacional.

2 ÁMBITO DE APLICACIÓN DEL MECANISMO DE CERTIFICACIÓN Y OBJETIVO DE EVALUACIÓN

a. ¿Se ha descrito con claridad el ámbito de aplicación del mecanismo de certificación (para el cual se deberán utilizar los criterios relativos a la protección de datos)?

b. ¿El ámbito de aplicación del mecanismo de certificación es significativo y no resulta engañoso para su público objetivo?

- *Ejemplo: Un «Sello de Empresa de Confianza» sugiere que se han auditado las actividades de tratamiento de toda una empresa, a pesar de que, en realidad, solo son objeto de certificación las operaciones de tratamiento especificadas, por ejemplo, el proceso de pago en línea. El ámbito de aplicación es, por lo tanto, engañoso.*

c. ¿El ámbito de aplicación del mecanismo de certificación refleja todos los aspectos relevantes de las operaciones de tratamiento?

- *Ejemplo: Una «Marca Sanitaria de Privacidad» debe incluir todos los datos de evaluación relativos a la salud con el fin de cumplir los requisitos previstos en el artículo 9.*

d. ¿El ámbito de aplicación del mecanismo de certificación permite una certificación significativa en relación con la protección de datos teniendo en cuenta la naturaleza, el contenido y el riesgo de las operaciones de tratamiento relacionadas?

- *Ejemplo: Si el ámbito de aplicación del mecanismo de certificación se centra solo en los aspectos específicos de las operaciones de tratamiento, tales como la recogida de datos, pero no en las demás operaciones de tratamiento, tales como el tratamiento con el fin de crear perfiles de publicidad o la gestión de los derechos del interesado, no sería significativo para los interesados.*

e. ¿El ámbito de aplicación del mecanismo de certificación abarca el tratamiento de datos personales en el país donde se presenta la solicitud, o aborda el tratamiento o las transferencias transfronterizas?

f. ¿Los criterios de certificación ofrecen una descripción suficiente del modo en que debe definirse el objetivo de evaluación?

- *Ejemplo: Un «Sello de Privacidad» que ofrezca un ámbito de aplicación general que exija solamente «una especificación del tratamiento sujeto a certificación» no ofrecería una orientación suficientemente clara sobre cómo establecer y describir un objetivo de evaluación.*
- *Ejemplo: Un ámbito de aplicación (específico), «El Sello de Bóveda de Privacidad», que trata el almacenamiento seguro debe describir con detalle los requisitos para cumplir los criterios de este ámbito de aplicación, como son la definición de la bóveda, los requisitos del sistema y las medidas técnicas y organizativas obligatorias. En ese caso, el ámbito de aplicación puede definir claramente el objetivo de evaluación.*

(1) ¿Los criterios requieren que el objetivo de evaluación incluya una identificación de todas las operaciones de tratamiento pertinentes, la ilustración de los flujos de datos y una determinación del área de aplicación del objetivo de evaluación?

- *Ejemplo: Un mecanismo de certificación ofrece la certificación de las operaciones de tratamiento de los responsables del tratamiento en virtud del RGPD sin especificar adicionalmente el área de aplicación (ámbito de aplicación general). Los criterios utilizados por el mecanismo requieren que el responsable del tratamiento de datos determine la operación de tratamiento específica (objetivo de evaluación) en lo que se refiere a los tipos de datos, los sistemas y los procesos desplegados.*

(2) ¿Los criterios requieren que el solicitante deje claro dónde empieza y dónde termina el tratamiento que está sujeto a evaluación? ¿Los criterios requieren que el objetivo de evaluación incluya interfaces en las que no estén incluidas las operaciones de tratamiento interdependientes como parte del objetivo de evaluación? ¿Y esto se justifica de manera satisfactoria?

- *Ejemplo: Un objetivo de evaluación que describe con suficientes detalles la operación de tratamiento de un servicio basado en la web, como la inclusión del registro de los usuarios, la prestación del servicio, la facturación, el registro de direcciones IP y las interfaces para usuarios y para terceros, pero no el alojamiento en el servidor (aunque incluyendo los contratos de tratamiento y los relativos a las medidas técnicas y organizativas).*

g. ¿Los criterios garantizan que los objetivos de evaluación (individuales) son comprensibles para el público destinatario, incluyendo a los interesados cuando proceda?

3 REQUISITOS GENERALES

a. ¿Se utilizan, identifican, explican y describen todos los términos pertinentes utilizados en el catálogo de criterios (es decir, la totalidad de los criterios de certificación)?

b. ¿Se identifican todas las referencias normativas?

c. ¿Los criterios incluyen la definición de las responsabilidades relativas a la protección de datos, los procedimientos y el tratamiento que abarca el ámbito de aplicación del mecanismo de certificación?

4 OPERACIÓN DE TRATAMIENTO, ARTÍCULO 42, APARTADO 1

Con respecto al ámbito de aplicación del mecanismo de certificación (general o específico), ¿los criterios abordan todos los componentes pertinentes de las operaciones de tratamiento (datos, sistemas y procesos)?

a. ¿Los criterios requieren la identificación de las bases jurídicas válidas de tratamiento con respecto al objetivo de evaluación?

b. Con respecto al objetivo de evaluación, ¿los criterios reconocen las fases pertinentes del tratamiento y el ciclo de vida completo de los datos, incluida la eliminación o la anonimización?

c. Con respecto al objetivo de evaluación, ¿los criterios requieren la portabilidad de los datos?

d. Con respecto al objetivo de evaluación, ¿los criterios permiten identificar y reflejar tipos especiales de operaciones de tratamiento, como las decisiones automatizadas o la elaboración de perfiles?

e. Con respecto al objetivo de evaluación, ¿los criterios permiten identificar categorías especiales de datos?

f. ¿Los criterios permiten y requieren la evaluación del riesgo de las operaciones de tratamiento individuales y las necesidades de protección de los derechos y las libertades de los interesados?

g. ¿Los criterios permiten y requieren una consideración adecuada de los riesgos que pueden sufrir los derechos y las libertades de las personas físicas?

…

5 LICITUD DEL TRATAMIENTO

a. ¿Los criterios requieren la comprobación de la licitud del tratamiento de las operaciones de tratamiento individuales con respecto a la finalidad y la necesidad de este?

b. ¿Los criterios requieren la comprobación de todos los requisitos de una base jurídica relativos a las operaciones de tratamiento individuales?

6 PRINCIPIOS, ARTÍCULO 5

a. ¿Los criterios abordan adecuadamente los principios de protección de datos con arreglo al artículo 5?

b. ¿Los criterios requieren demostración de la minimización de datos para cada uno de los objetivos de evaluación?

…

7 OBLIGACIONES GENERALES DE LOS RESPONSABLES Y LOS ENCARGADOS DEL TRATAMIENTO

a. ¿Los criterios requieren la prueba de los acuerdos contractuales formalizados entre los encargados y los responsables del tratamiento?

b. ¿Los acuerdos de los responsables y los encargados del tratamiento son objeto de evaluación?

c. ¿Los criterios reflejan las obligaciones del responsable del tratamiento con arreglo al capítulo IV?

d. ¿Los criterios requieren prueba de revisión y actualización de las medidas técnicas y organizativas aplicadas por el responsable del tratamiento con arreglo al artículo 24, apartado 1?

e. ¿Los criterios verifican que la organización ha evaluado si debe nombrarse un delegado de protección de datos (DPD) como exige el artículo 37? En su caso, ¿el DPD cumple los requisitos previstos en los artículos 37 a 39?

f. ¿Los criterios verifican que los registros del tratamiento de las actividades son necesarios de conformidad con el artículo 30, apartado 5, y que abordan de forma adecuada los requisitos del artículo 30?

8 DERECHOS DE LOS INTERESADOS

a. ¿Los criterios abordan adecuadamente el derecho de los interesados a la información y requieren que se pongan en marcha las medidas correspondientes?

b. ¿Los criterios requieren que se garantice a los interesados un acceso adecuado o incluso mayor y un control de sus datos, incluida la portabilidad de estos?

c. ¿Los criterios requieren que se pongan en marcha medidas que prevean la posibilidad de intervenir en la operación de tratamiento con el fin de garantizar los derechos de los interesados y permitir correcciones, supresiones o restricciones?

…

9 RIESGOS PARA LOS DERECHOS Y LAS LIBERTADES DE LAS PERSONAS FÍSICAS

a. ¿Los criterios permiten y requieren evaluar el riesgo que corren los derechos y las libertades de las personas físicas?

b. ¿Los criterios ofrecen o requieren una metodología de evaluación de riesgos reconocida? En su caso, ¿es acorde?

c. ¿Los criterios permiten y requieren la evaluación del efecto de las operaciones de tratamiento previstas para garantizar los derechos y las libertades de las personas físicas?

d. ¿Los criterios requieren consulta previa respecto a los riesgos restantes que no pudieron mitigarse, sobre la base de los resultados de la evaluación de impacto relativa a la protección de datos?

10 MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA PROTECCIÓN

a. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas que establezcan la confidencialidad de las operaciones de tratamiento?

b. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas que establezcan la integridad de las operaciones de tratamiento?

c. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas que establezcan la disponibilidad de las operaciones de tratamiento?

d. ¿Los criterios requieren la aplicación de medidas que establezcan la transparencia de las operaciones de tratamiento con respecto a...?

e. ¿La rendición de cuentas?

f. ¿Los derechos de los interesados?

g. ¿La evaluación de las operaciones de tratamiento individuales, por ejemplo, para la transparencia algorítmica?

h. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas que garanticen los derechos de los interesados, como la capacidad de proporcionar información o la portabilidad de los datos?

i. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas que establezcan la capacidad de intervenir en la operación de tratamiento con el fin de garantizar los derechos de los interesados y permitir correcciones, supresiones o restricciones?

j. ¿Los criterios requieren la aplicación de medidas que establezcan la posibilidad de intervenir en la operación de tratamiento con el fin de enmendar o comprobar el sistema o el proceso?

k. ¿Los criterios requieren la aplicación de medidas técnicas y organizativas para garantizar la minimización de datos, por ejemplo, la desvinculación o la separación de los datos del interesado, la anonimización, la seudonimización o el aislamiento de los sistemas de datos?

l. ¿Los criterios requieren medidas técnicas para aplicar los principios de la protección de datos por defecto?

m. ¿Los criterios requieren medidas técnicas y organizativas para aplicar los principios de la protección de datos desde el diseño, por ejemplo, un sistema de gestión de protección de datos para demostrar, informar, controlar y hacer cumplir los requisitos de protección de datos?

n. ¿Los criterios requieren medidas técnicas y organizativas para ejecutar actividades formativas y educativas periódicas y adecuadas destinadas al personal que tiene acceso permanente o habitual a los datos personales?

o. ¿Los criterios requieren la revisión de las medidas?

p. ¿Los criterios requieren autoevaluación/auditoría interna?

q. ¿Los criterios requieren medidas para garantizar que se llevan a cabo las obligaciones de notificación sobre violaciones de la seguridad de los datos personales a su debido tiempo y dentro del ámbito de aplicación pertinente?

r. ¿Los criterios requieren que los procedimientos de gestión de incidentes se apliquen y se verifiquen?

s. ¿Los criterios requieren un control de la evolución de los aspectos relativos a la intimidad y la tecnología, así como una actualización del sistema según se requiera?

…

11 OTRAS CARACTERÍSTICAS ESPECIALES FAVORABLES A LA PROTECCIÓN DE DATOS

a. ¿Los criterios requieren la aplicación de técnicas de mejora de la protección de datos? Esto podría incluir criterios que requieren una protección de datos mejorada mediante la eliminación o la reducción de los datos personales o del riesgo para la protección de datos.

- *Ejemplo: Los criterios que requieren una mejora de la imposibilidad de vinculación mediante el uso de la gestión de la identidad centrada en el usuario, tales como el uso de credenciales basadas en atributos durante la gestión de la identidad centrada en la organización, reflejarían una técnica de protección de datos mejorada.*

b. ¿Los criterios requieren la aplicación de controles mejorados de los interesados para facilitar la libre determinación y la elección?

…

12 CRITERIOS PARA DEMOSTRAR LA EXISTENCIA DE LAS GARANTÍAS ADECUADAS PARA LA TRANSFERENCIA DE LOS DATOS PERSONALES

Los criterios se abordarán en las próximas directrices sobre el artículo 42, apartado 2.

13 CRITERIOS ADICIONALES PARA UN SELLO EUROPEO DE PROTECCIÓN DE DATOS

a. ¿Los criterios prevén abarcar a todos los Estados miembros?

b. ¿Los criterios son capaces de tener en cuenta la legislación o los supuestos en materia de protección de datos de los Estados miembros?

c. ¿Los criterios requieren una evaluación de cada uno de los objetivos de evaluación con respecto a la legislación en materia de protección de datos sectorial concreta de un Estado miembro?

d. ¿Los criterios requieren que el responsable y el encargado del tratamiento ofrezcan información a los interesados y las partes interesadas en las lenguas de los Estados miembros...?

e. ¿Sobre el tratamiento/objetivo de evaluación?

f. ¿Sobre la documentación del tratamiento/objetivo de evaluación?

g. ¿Sobre los resultados de la evaluación?

…

14 EVALUACIÓN GLOBAL DE LOS CRITERIOS

a. ¿Los criterios abarcan el ámbito de aplicación del mecanismo de certificación al completo (es decir, todos los criterios) para ofrecer garantías suficientes y que la certificación sea fiable?

- *Ejemplo: Si el ámbito de aplicación del mecanismo de certificación se centra en las operaciones de tratamiento relacionadas con la salud, debe garantizarse un nivel elevado de protección de los datos mediante la definición de criterios que garanticen, por ejemplo,*

una evaluación en profundidad y la aplicación de los principios de protección de la intimidad desde el diseño y los principios de protección de la intimidad por defecto.

b. ¿Los criterios son acordes con el tamaño de la operación de tratamiento que aborda el ámbito de aplicación del mecanismo de certificación, la sensibilidad de la información y el riesgo de tratamiento?

c. ¿Los criterios tienen probabilidades de mejorar el cumplimiento de la protección de datos por parte de los responsables y los encargados del tratamiento?

d. ¿Los interesados se beneficiarán de sus derechos de información, que incluyen la explicación de los resultados deseados a los interesados?