Directrices 4/2018 relativas a la acreditación de los organismos de certificación conforme a lo dispuesto en el artículo 43 del Reglamento General de Protección de Datos (2016/679)

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 1 (versión 2.0 del anexo 1 adoptada el 4 de junio de 2019 después de la consulta pública)
Versión 2.0	4 de diciembre de 2018	Adopción de las directrices después de la consulta pública - En la misma fecha se adoptó el anexo 1 (versión 1.0) para consulta pública
Versión 1.0	6 de febrero de 2018	Adopción de las directrices por el Grupo de trabajo del artículo 29 (versión para consulta pública). Esta versión fue aprobada por el CEPD el 25 de mayo de 2018

Índice

TOC

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,

Habiendo considerado los resultados de la consulta pública sobre las directrices, que tuvo lugar en febrero de 2018, y sobre el anexo, que tuvo lugar entre el 14 de diciembre de 2018 y el 1 de febrero de 2019, como dispone el artículo 70, apartado 4, del Reglamento General de Protección de Datos

HA ADOPTADO LAS SIGUIENTES DIRECTRICES

1 INTRODUCCIÓN

1. El Reglamento General de Protección de Datos [Reglamento (UE) 2016/679] (en lo sucesivo, «el RGPD»), que entra en vigor el 25 de mayo de 2018, ofrece un marco de cumplimiento modernizado para la protección de datos en Europa, basado en la asunción de responsabilidades y en los derechos fundamentales. Para este nuevo marco, es fundamental disponer de una serie de medidas que faciliten el cumplimiento de las disposiciones del RGPD. Dichas medidas incluyen los requisitos obligatorios en circunstancias específicas (incluida la designación de delegados de protección de datos y la realización de evaluaciones de impacto relativas a la protección de datos) y medidas voluntarias, como códigos de conducta y mecanismos de certificación.

2. En el marco del establecimiento de mecanismos de certificación y de los sellos y marcas de protección de datos, el artículo 43, apartado 1, del RGPD exige a los Estados miembros que garanticen que los organismos de certificación que expiden la certificación contemplada en el artículo 42, apartado 1, estén acreditados por la autoridad de control competente o por el organismo nacional de acreditación, o por ambos. Si el organismo nacional de acreditación es el que realiza la acreditación de conformidad con lo dispuesto en la norma ISO/IEC 17065/2012, deberán aplicarse también los requisitos adicionales establecidos por la autoridad de control competente.

3. Los mecanismos de certificación adecuados pueden mejorar el cumplimiento del RGPD y la transparencia para los interesados y en las relaciones entre empresas (B2B), por ejemplo, entre responsables del tratamiento y encargados del tratamiento. Los responsables del tratamiento y los encargados del tratamiento se beneficiarán de una certificación independiente de terceros con el fin de demostrar el cumplimiento de sus operaciones de tratamiento[1].

[1] El considerando 100 del RGPD dispone que el establecimiento de mecanismos de certificación puede reforzar la transparencia y el cumplimiento del Reglamento y permitir a los interesados evaluar el nivel de protección de datos de los productos y servicios correspondientes.

4. En este contexto, el Comité Europeo de Protección de Datos (CEPD) reconoce que es necesario facilitar directrices en relación con la acreditación. El valor particular y la finalidad de la acreditación radican en el hecho de que ofrece una declaración fidedigna de la competencia de los organismos de certificación que permite generar confianza en el mecanismo de certificación.

5. El objetivo de las directrices es ofrecer orientación sobre cómo interpretar y aplicar las disposiciones del artículo 43 del RGPD. En particular, su objetivo es ayudar a los Estados miembros, a las autoridades de control y a los organismos nacionales de acreditación a establecer una base uniforme y armonizada para la acreditación de los organismos de certificación que expiden la certificación de conformidad con el RGPD.

2 ÁMBITO DE APLICACIÓN DE LAS DIRECTRICES

6. Las presentes directrices:

- establecen la finalidad de la acreditación en el contexto del RGPD;
- explican las vías disponibles para acreditar a los organismos de certificación de conformidad con el artículo 43, apartado 1, e identifican las cuestiones clave que deben tenerse en cuenta;
- ofrecen un marco para establecer requisitos de acreditación adicionales cuando el organismo nacional de acreditación se encargue de llevar a cabo la acreditación; y
- ofrecen un marco para establecer los requisitos de acreditación cuando la autoridad de control se encargue de llevar a cabo la acreditación.

7. Las directrices no son un manual de procedimiento para la acreditación de los organismos de certificación de conformidad con el RGPD. No desarrollan una nueva norma técnica para la acreditación de los organismos de certificación a efectos del RGPD.

8. Las directrices se dirigen a:

- los Estados miembros, que deben garantizar que los organismos de certificación estén acreditados por la autoridad de control o el organismo nacional de acreditación;
- los organismos nacionales de acreditación que lleven a cabo la acreditación de los organismos de certificación con arreglo a lo dispuesto en artículo 43, apartado 1, letra b);
- la autoridad de control competente que especifica «requisitos adicionales» a los de la norma ISO/IEC 17065/2012[2] cuando la acreditación la lleve a cabo el organismo nacional de acreditación con arreglo al artículo 43, apartado 1, letra b);
- el CEPD, cuando emite un dictamen y aprueba requisitos de acreditación de la autoridad de control competente de conformidad con el artículo 43, apartado 3, el artículo 70, apartado 1, letra p), y el artículo 64, apartado 1, letra c);
- la autoridad de control competente que especifica los requisitos de acreditación cuando la autoridad de control lleve a cabo la acreditación con arreglo al artículo 43, apartado 1, letra a);

[2] Organización Internacional de Normalización: Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.

- otras partes interesadas, como pueden ser posibles organismos de certificación o los propietarios de esquemas de certificación que facilitan criterios y procedimientos de certificación[3].

9. Definiciones

10. El objetivo de las siguientes definiciones es promover una interpretación común de los elementos básicos del proceso de acreditación. Deben considerarse puntos de referencia y no pretenden ser incuestionables. Estas definiciones se basan en los marcos regulatorios y normas existentes, especialmente en las disposiciones pertinentes del RGPD y en la norma ISO/IEC 17065/2012.

11. A efectos de las presentes directrices, se aplicarán las siguientes definiciones:

12. «*acreditación*» de los organismos de certificación, véase el apartado 3 relativo la interpretación de la acreditación a los efectos del artículo 43 del RGPD;

13. «*requisitos adicionales*» significa los requisitos establecidos por la autoridad de control competente y con respecto a los cuales se realiza una acreditación[4];

14. «*certificación*» significará la evaluación y la certificación imparcial por terceros [5] de que se ha demostrado el cumplimiento de los criterios de certificación;

15. «*organismo de certificación*» significará un organismo tercero[6] de evaluación de la conformidad[7] que explota mecanismos de certificación[8];

16. «*esquema de certificación*» significará un esquema de certificación relacionado con productos, procesos y servicios especificados a los que se aplican los mismos requisitos especificados, normas específicas y procedimientos[9];

17. «criterios» o criterios de certificación significará los criterios con arreglo a los cuales se lleva a cabo una certificación (evaluación de la conformidad);[10]

---

[3] El propietario del esquema es una organización identificable que ha establecido criterios de certificación y los requisitos para evaluar la conformidad. La organización que realiza las evaluaciones es la responsable de la acreditación (artículo 43, apartado 4) con arreglo a los requisitos del esquema de certificación y expide los certificados (es decir, el organismo de certificación, también conocido como organismo de evaluación de la conformidad). La organización que lleva a cabo las evaluaciones podría ser la misma que ha desarrollado y es propietaria del esquema, pero podría haber disposiciones en las que una organización es la propietaria del esquema y otra (o más de una) lleva a cabo las evaluaciones.

[4] Artículo 43, apartados 1, 3 y 6.

[5] Debe tenerse en cuenta que, de acuerdo con lo dispuesto en la norma ISO 17000, la certificación de terceros es «aplicable a todos los objetos de la evaluación de la conformidad» (5.5) «excepto a los propios organismos de evaluación de la conformidad, a los que es aplicable la acreditación» (5.6).

[6] La actividad de evaluación de la conformidad por terceros está a cargo de una organización independiente de la persona u organización que proporciona el objeto y de los intereses del usuario en ese objeto, véase la norma ISO 17000, 2.4.

[7] Véase la norma ISO 17000, 2.5: «organismo que presta servicios de evaluación de la conformidad»; ISO 17011: «organismo que presta servicios de evaluación de la conformidad y que puede ser objeto de acreditación»; ISO 17065, 3.12.

[8] Artículo 42, apartados 1 y 5, del RGPD.

[9] Véase el apartado 3.9 junto con el anexo B de la norma ISO 17065.

[10] Véase el artículo 42, apartado 5.

18. «organismo nacional de acreditación» significará el único organismo de un Estado miembro designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo con potestad pública para llevar a cabo acreditaciones[11].

3 INTERPRETACIÓN DE «ACREDITACIÓN» A EFECTOS DEL ARTÍCULO 43 DEL RGPD

19. El RGPD no define el término «acreditación». El artículo 2, apartado 10, del Reglamento (CE) n.º 765/2008, por el que se establecen los requisitos generales de acreditación, define la acreditación como

20. «declaración por un organismo nacional de acreditación de que un organismo de evaluación de la conformidad cumple los requisitos fijados con arreglo a normas armonizadas y, cuando proceda, otros requisitos adicionales, incluidos los establecidos en los esquemas sectoriales pertinentes, para ejercer actividades específicas de evaluación de la conformidad».

21. Según la norma ISO/IEC 17011

22. «acreditación se refiere a la declaración de un tercero, relativa a un organismo de evaluación de la conformidad, que demuestra formalmente su competencia para desempeñar funciones específicas de evaluación de la conformidad».

23. El artículo 43, apartado 1, establece:

24. «Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

    (a) la autoridad de control que sea competente en virtud del artículo 55 o 56;
    (b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo con arreglo a la norma ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56».

25. Por lo que respecta al RGPD, los requisitos de acreditación se guiarán por:

- la norma ISO/IEC 17065/2012 y los «requisitos adicionales» establecidos por la autoridad de control competente de conformidad con el artículo 43, apartado 1, letra b), cuando la acreditación la lleve a cabo el organismo nacional de acreditación y por la autoridad de control, cuando sea ella la que lleva a cabo la acreditación.

26. En ambos casos, los requisitos consolidados deben incluir los requisitos mencionados en el artículo 43, apartado 2.

[11] Véase el artículo 2, apartado 11, del Reglamento 765/2008/CE.

27. El CEPD reconoce que el propósito de la acreditación es proporcionar una declaración fidedigna de la competencia de un organismo para llevar a cabo la certificación (actividades de evaluación de la conformidad)[12]. En el sentido del RGPD, se entenderá que acreditación significa lo siguiente:

28. una declaración[13] realizada por un organismo nacional de acreditación o por una autoridad de control, de que un organismo de certificación[14] está cualificado para llevar a cabo la certificación de conformidad con los artículos 42 y 43 del RGPD, teniendo en cuenta la norma ISO/IEC 17065/2012 y los requisitos adicionales establecidos por la autoridad de control o por el Comité.

4 ACREDITACIÓN DE CONFORMIDAD CON EL ARTÍCULO 43, APARTADO 1, DEL RGPD

29. El artículo 43, apartado 1, reconoce que existen varias opciones para la acreditación de los organismos de certificación. El RGPD exige a las autoridades de control y a los Estados miembros que definan el proceso de acreditación de los organismos de certificación. En este apartado se recogen las vías de acreditación previstas en el artículo 43.

4.1 Función de los Estados miembros

30. El artículo 43, apartado 1, exige a los Estados miembros que *garanticen* que los organismos de certificación están acreditados, pero permite a cada Estado miembro determinar quién debe ser responsable de llevar a cabo la evaluación que da lugar a la acreditación. Con arreglo a lo dispuesto en el artículo 43, apartado 1, existen tres opciones; la acreditación la lleva a cabo:

(1) exclusivamente la autoridad de control, sobre la base de sus propios requisitos;
(2) exclusivamente el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) 765/2008 y sobre la base de la norma ISO/IEC 17065/2012 y de los requisitos adicionales establecidos por la autoridad de control competente; o
(3) la autoridad de control y el organismo nacional de acreditación (y de conformidad con todos los requisitos enumerados en el punto 2 anterior).

31. Corresponde a cada Estado miembro decidir si el organismo nacional de acreditación o la autoridad de control, o ambos conjuntamente, llevarán a cabo estas actividades de acreditación, pero en cualquier caso debe garantizar que se proporcionan los recursos adecuados[15].

4.2 Interacción con el Reglamento (CE) 765/2008

32. El CEPD señala que el artículo 2, apartado 11, del Reglamento (CE) n.º 765/2008 define a un organismo nacional de acreditación como «el *único* organismo de un Estado miembro con potestad pública para llevar a cabo acreditaciones».

---

[12] Véase el considerando 15 del Reglamento 765/2008/CE.
[13] Véase el artículo 2, apartado 10, del Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos.
[14] Véase la definición del término «acreditación» según la norma ISO 17011.
[15] Véase el artículo 4, apartado 9, del Reglamento (CE) 765/2008.

33. El artículo 2, apartado 11, podría considerarse incompatible con el artículo 43, apartado 1, del RGPD, que permite la acreditación por un organismo distinto del organismo nacional de acreditación del Estado miembro. El CEPD considera que la intención de la legislación de la UE ha sido no aplicar el principio general de que la acreditación sea realizada exclusivamente por la autoridad nacional de acreditación, otorgando a las autoridades de control la misma potestad en lo que respecta a la acreditación de los organismos de certificación. Por tanto, el artículo 43, apartado 1, es *lex specialis* en relación con el artículo 2, apartado 11, del Reglamento 765/2008.

4.3 Función del organismo nacional de acreditación:

34. El artículo 43, apartado 1, letra b), establece que el organismo nacional de acreditación acreditará a los organismos de certificación con arreglo a la norma ISO/IEC 17065/2012 y los requisitos adicionales establecidos por la autoridad de control competente.

35. En aras de la claridad, el CEPD señala que la referencia específica al artículo 43, apartado 3, letra b), del primer párrafo, implica que «tales requisitos» se refieren a los «requisitos adicionales» establecidos por la autoridad de control competente con arreglo al artículo 43, apartado 1, letra b), y a los requisitos establecidos en el artículo 43, apartado 2.

36. En el proceso de acreditación, los organismos nacionales de acreditación aplicarán los requisitos adicionales que deben facilitar las autoridades de control.

37. Un organismo de certificación con acreditación existente sobre la base de la norma ISO/IEC 17065/2012 para esquemas de certificación no relacionados con el RGPD que desee ampliar el alcance de su acreditación para cubrir la certificación expedida de acuerdo con el RGPD deberá cumplir los requisitos adicionales establecidos por la autoridad de control si el organismo nacional de acreditación se encarga de la acreditación. Si la acreditación para la certificación en virtud del RGPD la ofrece únicamente la autoridad de control competente, un organismo de certificación que solicite la acreditación deberá cumplir los requisitos establecidos por la autoridad de control correspondiente.

4.4 Función de la autoridad de control

38. El CEPD señala que el artículo 57, apartado 1, letra q), establece que *incumbirá* a la autoridad de control efectuar la acreditación de organismos de certificación con arreglo al artículo 43 como «tarea de la autoridad de control» de conformidad con el artículo 57 y el artículo 58, apartado 3, letra e), establece que la autoridad de control dispone de los poderes correctivos para acreditar a los organismos de certificación de conformidad con el artículo 43. El texto del apartado 1 del artículo 43 ofrece cierta flexibilidad y la función de acreditación de la autoridad de control debe interpretarse como una tarea únicamente cuando proceda. El Derecho del Estado miembro puede utilizarse para aclarar este punto. Ahora bien, en el proceso de acreditación por parte de un organismo nacional de acreditación, el organismo de certificación está obligado, en virtud del artículo 43, apartado 2, letra a), a demostrar su independencia y su pericia a satisfacción de la autoridad de control competente en relación con el objeto del mecanismo de certificación que ofrece[16].

39. Si un Estado miembro estipula que los organismos de certificación deben estar acreditados por la autoridad de control, esta deberá establecer requisitos de acreditación, incluidos, sin

[16] Los requisitos adicionales establecidos por la autoridad de control con arreglo al artículo 43, apartado 1, letra b), deberán especificar los requisitos de independencia y pericia. Véase también el anexo 1 de las directrices.

ánimo limitativo, los requisitos enumerados en el artículo 43, apartado 2. En comparación con las obligaciones relativas a la acreditación de los organismos de certificación por los organismos nacionales de acreditación, el artículo 43 ofrece menos instrucciones sobre los requisitos de acreditación cuando es la propia autoridad de control la que lleva a cabo la acreditación. Para contribuir a la adopción de un enfoque armonizado de la acreditación, los criterios de acreditación utilizados por la autoridad de control deben guiarse por la norma ISO/IEC 17065 y complementarse con los requisitos adicionales que establezca la autoridad de control de conformidad con el artículo 43, apartado 1, letra b). El CEPD señala que el artículo 43, apartado 2, letras a) a e), refleja y especifica los requisitos de la norma ISO 17065, lo que contribuirá a la coherencia.

40. Si un Estado miembro estipula que los organismos de certificación deben estar acreditados por los organismos nacionales de acreditación, la autoridad de control debe establecer requisitos adicionales que complementen los convenios de acreditación existentes previstos en el Reglamento (CE) 765/2008 (en el que los artículos 3 a 14 se refieren a la organización y el funcionamiento de la acreditación de los organismos de evaluación de la conformidad) y las normas técnicas que describen los métodos y los procedimientos de los organismos de certificación. A la luz de lo anterior, el Reglamento (CE) 765/2008 ofrece orientaciones adicionales: el artículo 2, apartado 10, define la acreditación y hace referencia a «normas armonizadas» y a los «requisitos adicionales, incluidos los establecidos en los esquemas sectoriales pertinentes». De ello se deduce que los requisitos adicionales establecidos por la autoridad de control deben incluir requisitos específicos y centrarse en facilitar la evaluación, entre otros aspectos, de la independencia y el nivel de pericia en materia de protección de datos de los organismos de certificación, por ejemplo, su capacidad para evaluar y certificar las operaciones de tratamiento de datos personales por parte de los responsables del tratamiento y de los encargados del tratamiento con arreglo al artículo 42, apartado 1. Esto incluye la competencia necesaria para los esquemas sectoriales y en relación con la protección de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de datos personales[17]. El anexo a las presentes directrices puede ayudar a orientar a las autoridades de control competentes a la hora de establecer los «requisitos adicionales» de conformidad con el artículo 43, apartado 1, letra b), y el artículo 43, apartado 3.

41. El artículo 43, apartado 6, establece que «la autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se a refiere el artículo 42, apartado 5, en una forma fácilmente accesible». Por consiguiente, para garantizar la transparencia, se publicarán todos los criterios y requisitos aprobados por una autoridad de control. En términos de calidad y confianza en los organismos de certificación, sería conveniente que el público pudiera acceder fácilmente a todos los requisitos de acreditación.

4.5 Autoridad de control que actúa como organismo de certificación

42. El artículo 42, apartado 5, establece que una autoridad de control podrá expedir certificaciones, pero el RGPD no exige que esté acreditada para cumplir los requisitos del Reglamento (CE) 765/2008. El CEPD señala que el artículo 43, apartado 1, letra a), y en concreto el artículo 58, apartado 2, letra h) y el apartado 3, letras a) y e) a f), facultan a las autoridades de control para que lleven a cabo tanto la acreditación como la certificación y, al

[17] Artículo 1, apartado 2 del RGPD.

mismo tiempo, presten asesoramiento y, en su caso, retiren certificaciones u ordenen a organismos de certificación que no expidan certificaciones.

43. Pueden darse situaciones en las que la separación de funciones y obligaciones de acreditación y certificación sea apropiada o necesaria, por ejemplo, si una autoridad de control y otros organismos de certificación coexisten en un Estado miembro y ambos expiden la misma gama de certificaciones. Por consiguiente, las autoridades de control deben adoptar medidas organizativas suficientes para separar las tareas del RGPD con el fin de afianzar y facilitar los mecanismos de certificación, adoptando, al mismo tiempo, precauciones para evitar conflictos de intereses que puedan derivarse de estas tareas. Asimismo, los Estados miembros y las autoridades de control deben tener en cuenta el nivel europeo armonizado a la hora de formular leyes y procedimientos nacionales relativos a la acreditación y la certificación de conformidad con el RGPD.

4.6 Requisitos de acreditación

44. En el anexo de las presentes directrices se ofrece información orientativa sobre cómo identificar requisitos adicionales de acreditación. Identifica las disposiciones pertinentes del RGPD y sugiere los requisitos que las autoridades de control y los organismos nacionales de acreditación deben tener en cuenta para garantizar el cumplimiento del RGPD.

45. Tal y como se ha expuesto anteriormente, cuando los organismos de certificación estén acreditados por el organismo nacional de acreditación de conformidad con el Reglamento (CE) 765/2008, la norma ISO/IEC 17065/2012 será la norma de acreditación pertinente complementada por los requisitos adicionales establecidos por la autoridad de control. El artículo 43, apartado 2, refleja las disposiciones genéricas de la norma ISO/IEC 17065/2012 a la luz de la protección de los derechos fundamentales en virtud del RGPD. El marco del anexo utiliza el artículo 43, apartado 2, y la norma ISO/IEC 17065/2012 como base para la identificación de requisitos, así como otros criterios relativos a la evaluación de la pericia en materia de protección de datos de los organismos de certificación y su capacidad para respetar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales tal y como se establece en el RGPD. El CEPD señala que se centra especialmente en garantizar que los organismos de certificación dispongan de un nivel adecuado de pericia en materia de protección de datos, de conformidad con el artículo 43, apartado 1.

46. Los requisitos adicionales de acreditación establecidos por la autoridad de control se aplicarán a todos los organismos de certificación que soliciten la acreditación. El organismo de acreditación evaluará si dicho organismo de certificación es competente para llevar a cabo la actividad de certificación de acuerdo con los requisitos adicionales y el objeto de la certificación. Habrá referencias a sectores específicos o áreas de certificación para los que el organismo de certificación esté acreditado.

47. El CEPD también señala que se requiere pericia en materia de protección de datos, además de los requisitos de la ISO/IEC 17065/2012, si otros organismos externos, como laboratorios o auditores, llevan a cabo partes o componentes de actividades de certificación por cuenta de un organismo de certificación acreditado. En estos casos, la acreditación de estos organismos externos no es posible en virtud del RGPD. No obstante, con el fin de garantizar la idoneidad de estos organismos para su actividad por cuenta de los organismos de certificación acreditados, es necesario que el organismo de certificación acreditado garantice que la pericia en materia de protección de datos requerida para el organismo acreditado también debe

aplicarse y demostrarse en el caso del organismo externo con respecto a la actividad pertinente realizada.

48. El marco para identificar los requisitos adicionales de acreditación presentados en el anexo de las presentes directrices no constituye un manual de procedimiento para el proceso de acreditación realizado por el organismo nacional de acreditación o la autoridad de control. Ofrece orientaciones sobre la estructura y la metodología y, por tanto, un conjunto de herramientas a disposición de las autoridades de control para identificar los requisitos adicionales para la acreditación.

ANEXO 1

El anexo 1 ofrece orientaciones sobre los requisitos «adicionales» de acreditación con respecto a la norma ISO/IEC 17065/2012 y de conformidad con el artículo 43, apartado 1, letra b), y el artículo 43, apartado 3, del RGPD.

En el presente anexo se establecen los requisitos sugeridos que una autoridad de control de protección de datos elaborará y aplicará durante la acreditación de un organismo de certificación por el organismo nacional de acreditación o la autoridad de control competente[18]. Estos requisitos adicionales deben comunicarse al Comité Europeo de Protección de Datos antes de su aprobación conforme al artículo 64, apartado 1, letra c).

El presente anexo debe leerse en relación con la norma ISO/IEC 17065/2012. La numeración de los apartados utilizada en el anexo se corresponde con la utilizada en la norma ISO/IEC 17065/2012. Cuando las autoridades de control lleven a cabo una acreditación de conformidad con el artículo 43, apartado 1, letra a), sería conveniente que también la utilizaran cuando sea posible. Esto contribuirá a una acreditación armonizada en la UE.

Sin perjuicio de las siguientes orientaciones, o de que no haya orientaciones sobre algún punto de la norma ISO/IEC 17065/2012, la autoridad de control competente puede establecer otros requisitos adicionales relativos a estos puntos si son conformes a la legislación nacional.

0 PREFIJO

[El presente apartado trata de las condiciones de cooperación acordadas, si procede, entre el organismo nacional de acreditación y la autoridad de control de protección de datos, por ejemplo, quién debe ser responsable de recibir las solicitudes o cómo organizar el reconocimiento de los criterios aprobados como parte del proceso de acreditación.]

1 ÁMBITO DE APLICACIÓN[19]

El ámbito de aplicación de la norma ISO/IEC 17065/2012 se aplicará de conformidad con el RGPC. Las directrices sobre acreditación y certificación aportan más información. El ámbito de aplicación de un mecanismo de certificación (por ejemplo, operaciones de tratamiento de un servicio de computación en nube) debe tenerse en cuenta en la evaluación por el ONA y la autoridad de control competente durante el proceso de acreditación, especialmente en cuanto a los criterios, pericia y metodología de evaluación. El amplio ámbito de aplicación de la norma ISO/IEC 17065/2012 que abarca productos, procesos y servicios no debe ser inferior ni anular los requisitos del RGPD, por ejemplo, un mecanismo de gobernanza no puede ser el único elemento de un mecanismo de certificación, puesto que la certificación debe incluir el tratamiento de datos personales, es decir, operaciones de tratamiento. De conformidad con el artículo 42, apartado 1, del RGPD, la certificación solo es aplicable a las operaciones de tratamiento de los responsables y los encargados.

[18] Para más información sobre el proceso de aprobación de los requisitos de certificación, véase el apartado 4 de las directrices de certificación.
[19] La numeración remite a la norma ISO/IEC 17065/2012.

2 REFERENCIAS NORMATIVAS

El RGPD tiene prioridad sobre la norma ISO/IEC 17065/2012. Si en los requisitos adicionales o el mecanismo de certificación se hace referencia a otras normas ISO, estas se interpretarán en consonancia con los requisitos expuestos en el RGPD.

3 TÉRMINOS Y DEFINICIONES

En el presente anexo, se aplicarán los términos y definiciones de las directrices relativas a la acreditación (WP 261) y certificación (CEPD 1/2018) y prevalecerán sobre las definiciones ISO.

4 REQUISITOS GENERALES DE ACREDITACIÓN

4.1 Temas legales y contractuales

4.1.1 Responsabilidad legal

Un organismo de certificación debe poder demostrar (en todo momento) al ONA o al ARC que aplica procedimientos actualizados que demuestren el cumplimiento de las responsabilidades legales en el ámbito de la acreditación, incluidos los requisitos adicionales con respecto a la aplicación del Reglamento 2016/679/EC. Téngase en cuenta que, puesto que el propio organismo de certificación es responsable/encargado del tratamiento, podrá aportar pruebas de procedimientos y medidas conformes con el Reglamento 2016/679/CE específicamente para el control y tratamiento de los datos personales de la organización cliente como parte del proceso de certificación.

El ARC podrá decidir añadir otros requisitos y procedimientos para comprobar el cumplimiento del RGPD por parte de los organismos de certificación antes de la acreditación.

4.1.2 Acuerdo de certificación («AC»)

Los requisitos mínimos para un acuerdo de certificación se completarán con los puntos siguientes:

El organismo de certificación demostrará, además de los requisitos de la norma ISO/IEC 17065/2012, que sus acuerdos de certificación:

1. exigen que el solicitante cumpla siempre tanto los requisitos de certificación generales a tenor de 4.1.2.2 letra a) de la norma ISO/IEC 17065/2012 como los criterios aprobados por la autoridad de control competente o el CEPD de conformidad con el artículo 43, apartado 2, letra b), y del artículo 42, apartado 5;
2. exigen que el solicitante permita total transparencia a la autoridad de control competente con respecto al procedimiento de certificación, incluidas las cuestiones contractualmente confidenciales relativas al cumplimiento de la protección de datos con arreglo al artículo 42, apartado 7, y al artículo 58, apartado 1, letra c);
3. no reducen la responsabilidad del solicitante en cuanto al cumplimiento del Reglamento 2016/679/CE, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 42, apartado 5;
4. exigen al solicitante que facilite al organismo de certificación toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación con arreglo al artículo 42, apartado 6;
5. exigen al solicitante que respete los plazos y procedimientos aplicables. El acuerdo de certificación debe estipular que deben observarse y asumirse los plazos y los

procedimientos resultantes, por ejemplo, del programa de certificación o de otras reglamentaciones;

6. con respecto a 4.1.2.2 letra c), n.º 1 de la norma ISO/IEC 17065/2012 fijan las normas de validez, renovación y retirada con arreglo al artículo 42, apartado 7, y al artículo 43, apartado 4, incluidas las normas que fijan los intervalos apropiados de reevaluación o revisión (regularidad) con arreglo al artículo 42, apartado 7;
7. permiten al organismo de certificación revelar toda la información necesaria para conceder la certificación de conformidad con el artículo 42, apartado 8, y el artículo 43, apartado 5;
8. incluyen normas sobre las precauciones necesarias para la investigación de reclamaciones a tenor de 4.1.2.2 letra c), n.º 2, adicionalmente, letra j), contendrá también declaraciones explícitas sobre la estructura y el procedimiento para la tramitación de reclamaciones, de conformidad con el artículo 43, apartado 2, letra d);
9. además de los requisitos mínimos contemplados en 4.1.2.2 de la norma ISO/IEC 17065/2012, si las consecuencias de la retirada o la suspensión de la acreditación para el organismo de certificación afectan al cliente, en tal caso las consecuencias para el cliente también deben abordarse;
10. exigen que el solicitante informe al organismo de certificación en caso de cambios importantes en su situación real o jurídica y en sus productos, procesos y servicios a que se refiera a la certificación.

4.1.3 Uso de sellos y marcas de protección de datos

Los certificados, sellos y marcas de protección de datos solo se utilizarán de conformidad con el artículo 42 y el artículo 43 y con las directrices sobre acreditación y certificación.

4.2 Gestión de la imparcialidad

El organismo de acreditación garantizará que, además del requisito expuesto en 4.2. de la norma ISO/IEC 17065/2012,

1. el organismo de certificación cumple los requisitos adicionales establecidos por la autoridad de control competente [(de conformidad con el artículo 43, apartado 1, letra b)]
    a. con arreglo al artículo 43, apartado 2, letra a), aportará pruebas separadas de su independencia. Esto se aplica, en especial, a las pruebas relativas a la financiación del organismo de certificación en la medida en que se refieran a la garantía de imparcialidad;
    b. sus funciones y obligaciones no dan lugar a conflicto de intereses con arreglo al artículo 43, apartado 2, letra e);
2. el organismo de certificación no tiene ninguna relación relevante con el cliente al que evalúa.

4.3 Responsabilidad legal y financiación

El organismo de acreditación, además del requisito establecido en 4.3.1 de la norma ISO/IEC 17065/2012, garantizará con regularidad que el organismo de certificación cuenta con las medidas adecuadas (por ejemplo, seguros o reservas) para cubrir sus responsabilidades legales en las zonas geográficas en las que opera.

4.4 Condiciones de no discriminación

La autoridad de control podrá establecer requisitos adicionales si son conformes a la legislación nacional.

4.5 Confidencialidad

La autoridad de control podrá establecer requisitos adicionales si son conformes a la legislación nacional.

4.6 Información disponible al público

El organismo de acreditación exigirá al organismo de certificación, además del requisito establecido en 4.6 de la norma ISO/IEC 17065/2012 que, como mínimo:

1. todas las versiones (actuales y anteriores) de los criterios aprobados utilizados a tenor del artículo 42, apartado 5, se publiquen y sean fácilmente accesibles al público así como todos los procedimientos de certificación, generalmente estableciendo el periodo de validez respectivo;
2. la información sobre los procedimientos de tramitación de reclamaciones y los recursos se haga pública de conformidad con el artículo 43, apartado 2, letra d).

5 REQUISITOS RELATIVOS A LA ESTRUCTURA, ARTÍCULO 43, APARTADO 4 [«CORRECTA EVALUACIÓN»]

5.1 Estructura de la organización y alta dirección

La autoridad de control podrá establecer requisitos adicionales.

5.2 Mecanismos para salvaguardar la imparcialidad

La autoridad de control podrá establecer requisitos adicionales.

6 REQUISITOS PARA LOS RECURSOS

6.1 Personal del organismo de certificación

El organismo de acreditación garantizará, además del requisito establecido en el apartado 6 de la norma ISO/IEC 17065/2012, para cada organismo de certificación que su personal:

1. ha demostrado un nivel de pericia adecuado y permanente (conocimientos y experiencia) con respecto a la protección de datos de conformidad con el artículo 43, apartado 1;
2. tiene un nivel de pericia adecuado y permanente con respecto al objeto de la certificación con arreglo al artículo 43, apartado 2, letra e), y no tienen conflicto de intereses con arreglo al artículo 43, apartado 2, letra e);
3. se compromete a respetar los criterios mencionados en el artículo 42, apartado 5, con arreglo al artículo 43, apartado 2, letra b);
4. tiene conocimientos relevantes y adecuados en la aplicación de la legislación sobre protección de datos y experiencia al respecto;
5. tiene conocimientos relevantes y adecuados en medidas técnicas y organizativas de protección de datos y experiencia al respecto según proceda;
6. puede demostrar experiencia en los ámbitos mencionados en los requisitos adicionales establecidos en 6.1.1, 6.1.4, y 6.1.5, específicamente

Para el personal con pericia técnica:

- Haber obtenido una cualificación en un ámbito relevante de pericia técnico de nivel 6 como mínimo del Marco Europeo de Cualificaciones[20] o un título protegido reconocido (por ejemplo, Dipl. Ing.) en la correspondiente profesión regulada o tenga una dilatada experiencia profesional.
- Al *personal responsable de decisiones de certificación* se le exige una dilatada experiencia profesional en la identificación e implementación de medidas de protección de datos.
- Al *personal responsable de las evaluaciones* se le exige experiencia profesional en la protección de datos técnicos y conocimientos y experiencia en procedimientos comparables (por ejemplo certificaciones o auditorías), y estar registrado según proceda.

El personal demostrará que mantiene sus conocimientos técnicos y en materia de auditoría específicos de un campo mediante el desarrollo profesional continuado.

Para el personal con pericia jurídica:

- Estudios de Derecho en una universidad de la UE o reconocida por el Estado durante al menos ocho semestres, sancionados por el título de Máster en Abogacía o equivalente, o una dilatada experiencia profesional.
- El *personal responsable de las decisiones de certificación* demostrará una dilatada experiencia profesional en el Derecho de protección de datos y estará registrado como exija el Estado miembro.
- El *personal responsable de las evaluaciones* demostrará una experiencia profesional de dos años como mínimo en derecho de protección de datos y conocimientos y experiencia procedimientos comparables (por ejemplo certificaciones o auditorías), y estar registrado cuando lo exija el Estado miembro.
    - El personal demostrará que mantiene sus conocimientos técnicos y en materia de auditoría específicos de un campo mediante el desarrollo profesional continuado.

6.2 Recursos para la evaluación

La autoridad de control podrá establecer requisitos adicionales si son conformes a la legislación nacional.

7 REQUISITOS DEL PROCEDIMIENTO, ARTÍCULO 43, APARTADO 2, LETRAS C) Y D)

7.1 Generalidades

El organismo de acreditación deberá garantizar, además del requisito establecido en 7.1 de la norma ISO/IEC 17065/2012, lo siguiente:

1. que los organismos de certificación cumplen los requisitos adicionales establecidos por la autoridad de control competente [(de conformidad con el artículo 43, apartado 1, letra b)] al presentar la solicitud de manera que sus funciones y obligaciones no den lugar a conflicto de intereses con arreglo al artículo 43, apartado 2, letra b);
2. que notifiquen a las ARC antes de que el organismo de certificación comience a operar un Sello Europeo de Protección de Datos aprobado en un nuevo Estado miembro en una oficina auxiliar.

[20] Véase el comparador de cualificaciones en https://ec.europa.eu/ploteus/en/compare?

7.2 Solicitud

Además del punto 7.2 de la norma ISO/IEC 17065/2012, debe exigirse que:

1. el objeto de certificación (objetivo de evaluación) debe describirse con detalle en la solicitud; esto también incluye interfaces y transferencias a otros sistemas y organizaciones, protocolos y otros seguros;
2. la solicitud especificará si intervienen los encargados y, cuando los encargados sean el solicitante, se describirán sus responsabilidades y funciones y la solicitud contendrá los contratos relevantes del responsable/encargado.

7.3 Revisión de la solicitud

Además del punto 7.3 de la norma ISO/IEC 17065/2012, debe exigirse que:

1. en el acuerdo de certificación se expongan métodos de evaluación vinculantes con respecto al objetivo de evaluación;
2. la evaluación en 7.3(e) de si el nivel de pericia es suficiente tenga en cuenta tanto la pericia técnica como jurídica en la protección de datos en una medida adecuada.

7.4 Evaluación

Además del punto 7.4 de la norma ISO/IEC 17065/2012, los mecanismos de certificación describirán métodos de evaluación suficientes para evaluar el cumplimiento por parte de las operaciones de tratamiento de datos de los criterios de certificación, entre otros, por ejemplo, cuando sea aplicable:

1. un método para evaluar la necesidad y proporcionalidad de las operaciones de tratamiento con respecto a sus fines y a los interesados afectados;
2. un método para evaluar la cobertura, composición y evaluación de todos los riesgos contemplados por el responsable y el encargado del tratamiento con respecto a las consecuencias jurídicas de conformidad con los artículos 30, 32, 35 y 36 del RGPD, y con respecto a la definición de las medidas técnicas y organizativas de conformidad con los artículos 24, 25 y 32 del RGPD, puesto que los citados artículos se aplican al objeto de la certificación y
3. un método para evaluar los recursos, incluidas las garantías, salvaguardias y procedimientos para garantizar la protección de datos personales en el contexto del tratamiento que deba asignarse el objeto de certificación y demostrar que se cumplen los requisitos jurídicos establecidos en los criterios; y
4. documentación de los métodos y conclusiones.

Se exigirá al organismo de certificación que garantice que estos métodos de evaluación están normalizados y son de aplicación general. Esto significa que se utilizan métodos de evaluación comparables para objetivos de evaluación comparables. El organismo de certificación justificará cualquier desviación de este procedimiento.

Además del punto 7.4.2 de la norma ISO/IEC 17065/2012, debe permitirse que la evaluación sea realizada por peritos externos que hayan sido reconocidos por el organismo de certificación.

Además del punto 7.4.5 de la norma ISO/IEC 17065/2012, debe exigirse que la certificación de protección de datos con arreglo al artículo 42 y el artículo 43 del RGPD, que ya cubre parte del objeto de certificación, pueda incluirse en una certificación vigente. No obstante, no será suficiente para sustituir completamente evaluaciones (parciales). El organismo de certificación estará obligado a verificar el cumplimiento de los criterios. En cualquier caso, el reconocimiento requerirá la disponibilidad de un informe de evaluación completo o de información que permita una evaluación de

la actividad de certificación anterior y sus resultados. Una declaración de certificación o certificados similares de certificación no deben considerarse suficientes para sustituir a un informe.

Además del punto 7.4.6 de la norma ISO/IEC 17065/2012, debe exigirse que el organismo de certificación exponga con detalle en su mecanismo de certificación cómo informa al cliente (solicitante de la certificación) la información solicitada en el punto 7.4.6 de la no conformidad de un mecanismo de certificación. A este respecto, debe definirse como mínimo la naturaleza y el calendario de dicha información.

Además del punto 7.4.9 de la norma ISO/IEC 17065/2012, debe exigirse que la documentación esté totalmente accesible para la autoridad de control de protección de datos cuando esta la solicite

7.5 Revisión

Además del punto 7.5 de la norma ISO/IEC 17065/2012, se requieren procedimientos para la concesión, revisión regular y revocación de las certificaciones respectivas con arreglo al artículo 43, apartados 2 y 3.

7.6 Decisión de certificación

Además del punto 7.6.1 de la norma ISO/IEC 17065/2012, debe exigirse al organismo de certificación que exponga con detalle en sus procedimientos como se garantizan su independencia y responsabilidad con respecto a las decisiones de certificación individuales.

7.7 Documentación de certificación

Además del punto 7.7.1.e de la norma ISO/IEC 17065/2012 y de conformidad con el artículo 42, apartado 7, del RGPD, debe exigirse que el periodo de validez de las certificaciones no exceda de tres años.

Además del punto 7.7.1.e de la norma ISO/IEC 17065/2012, debe exigirse que también se documente el periodo de supervisión prevista a tenor de la sección 7.9.

Además del punto 7.7.1.f de la norma ISO/IEC 17065/2012, debe exigirse que el organismo de certificación haga constar el objeto de certificación en la documentación de certificación (declarando la situación de la versión o características similares, si procede).

7.8 Directorio de productos certificados

Además del punto 7.8 de la norma ISO/IEC 17065/2012, debe exigirse al organismo de certificación que conserve la información sobre productos, procesos y servicios certificados disponible interna y públicamente. El organismo de certificación facilitará al público un resumen del informe de evaluación. El objetivo de dicho resumen es contribuir a la transparencia sobre qué se ha certificado y cómo se ha evaluado. En él se explicarán, por ejemplo:

(a) el alcance de la certificación y una descripción significativa del objeto de certificación (objetivo de evaluación);

(b) los criterios respectivos de certificación (incluida la versión o situación funcional);

(c) los métodos de evaluación y las pruebas realizadas y

(d) los resultados.

Además del punto 7.8 de la norma ISO/IEC 17065/2012 y de conformidad con el artículo 45, apartado 5, del RGPD, el organismo de certificación informará a las autoridades de control competentes de las razones de la expedición de la certificación solicitada o de su retirada.

7.9 Vigilancia

Además de los puntos 7.9.1, 7.9.2 y 7.9.3 de la norma ISO/IEC 17065/2012, y de conformidad con el artículo 43, apartado 2, letra c), del RGPD, debe exigirse que sean obligatorias medidas regulares de supervisión para mantener la certificación durante el periodo de supervisión.

7.10 Cambios que afectan a la certificación

Además de los puntos 7.10.1 y 7.10.2 de la norma EN ISO/IEC 17065/2012, entre los cambios que afectan a la certificación que debe considerar el organismo de certificación están los siguientes: modificaciones de la legislación en materia de protección de datos, la adopción de actos delegados de la Comisión Europea de conformidad con el artículo 43, apartados 8 y 9, decisiones del Comité Europeo de Protección de Datos y decisiones de los órganos jurisdiccionales relativas a la protección de datos. Los procedimientos de cambio que se acuerden pueden incluir, entre otros: períodos transitorios, proceso de aprobación con la autoridad de control competente, reevaluación del objeto de certificación relevante y de las medidas adecuadas para revocar la certificación si la operación de tratamiento certificada ya no cumple los criterios actualizados.

7.11 Finalizar, reducir, suspender o retirar la certificación

Además del capítulo 7.11.1 de la norma ISO/IEC 17065/2012, debe exigirse al organismo de certificación que informe a la autoridad de control competente y al ONA cuando sea relevante inmediatamente por escrito de las medidas adoptadas y de la continuación, restricciones, suspensión y retirada de la certificación.

Según el artículo 58, apartado 2, letra h), se exigirá al organismo de certificación que acepte decisiones y órdenes de la autoridad de control competente para retirar o no expedir una certificación a un cliente (solicitante) si no se cumplen o dejan de cumplirse los requisitos para la certificación.

7.12 Registros

Debe exigirse al organismo de certificación que conserve toda la documentación completa, comprensible, actualizada y lista para la auditoría.

7.13 Reclamaciones y apelaciones, artículo 43, apartado 2, letra d)

Además del punto 7.13.1 de la norma ISO/IEC 17065/2012, debe exigirse al organismo de certificación que defina:

(a) quién puede presentar reclamaciones u objeciones;

(b) quién las tramita por parte del organismo de certificación;

(c) qué verificaciones se realizan en este contexto; y

(d) las posibilidades de consulta de las partes interesadas.

Además del punto 7.13.2 de la norma ISO/IEC 17065/2012, debe exigirse al organismo de certificación que defina:

(a) cómo y a quién debe darse esta confirmación;

(b) los plazos para ello; y

(c) qué procesos deben iniciarse después.

Además del punto 7.13.1 de la norma ISO/IEC 17065/2012, el organismo de certificación debe definir cómo se garantiza la separación entre las actividades de certificación y la tramitación de apelaciones y reclamaciones.

8 REQUISITOS DEL SISTEMA DE GESTIÓN

Según el capítulo 8 de la norma ISO/IEC 17065/2012, un requisito general del sistema de gestión es que la implementación de todos los requisitos de los capítulos anteriores dentro del ámbito de la aplicación del mecanismo de certificación por el organismo de certificación acreditado sea documentada, evaluada, controlada y supervisada independientemente.

El principio básico de gestión es definir un sistema según el cual sus objetivos se fijen con eficacia y eficiencia, específicamente: la implementación de los servicios de certificación, mediante especificaciones adecuadas. Esto requiere transparencia y verificabilidad de la implementación de los requisitos de acreditación por parte del organismo de certificación y su cumplimiento permanente.

Para ello, el sistema de gestión debe especificar una metodología para alcanzar y controlar estos requisitos en cumplimiento de la normativa de protección de datos y para que los controle permanentemente el propio organismo acreditado.

Estos principios de gestión y su implementación documentada deben ser transparentes y debe revelarlos el organismo de certificación acreditado con arreglo al procedimiento de acreditación y conforme al artículo 58 y, posteriormente, a petición de la autoridad de control de protección de datos, en cualquier momento durante una investigación en forma de revisiones de protección de datos en virtud del artículo 58, apartado 1, letra b), o una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7, de conformidad con el artículo 58, apartado 1, letra c).

En particular, el organismo de certificación acreditado debe hacer público de manera permanente y continuada qué certificaciones se han efectuado sobre qué base (o mecanismos o esquemas de certificación), cuánto tiempo son válidas las certificaciones en virtud de qué marco y condiciones (considerando 100).

8.1 Requisitos generales del sistema de gestión

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.2 Documentación del sistema de gestión

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.3 Control de documentos

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.4 Control de registros

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.5 Revisión por la dirección

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.6 Auditorías internas

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.7 Acciones correctivas

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

8.8 Acciones preventivas

La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

9 OTROS REQUISITOS ADICIONALES21

9.1 Actualización de los métodos de evaluación

El organismo de certificación establecerá procedimientos para orientar la actualización de los métodos de evaluación para la aplicación en el contexto de la evaluación en virtud con arreglo al punto 7.4. La actualización debe producirse en el curso de cambios en el marco jurídico, el riesgo o riesgos relevantes, el estado actual de la técnica y los costes de implementación de las medidas técnicas y organizativas.

9.2 Mantener las competencias

Los organismos de certificación establecerán procedimientos para garantizar la formación de sus empleados con vistas a actualizar sus competencias, teniendo en cuenta los cambios enumerados en el punto 9.1.

9.3 Responsabilidades y competencias

9.3.1 Comunicación entre el organismo de certificación y sus clientes

Deben existir procedimientos para implementar procedimientos adecuados y estructuras de comunicación entre el organismo de certificación y su cliente. Entre ellos:

1. Conservar la documentación de funciones y responsabilidades por parte del organismo de certificación acreditado, a efectos de:
    a. solicitudes de información, o
    b. hacer posible ponerse en contacto en caso de una reclamación sobre una certificación.
2. Conservar un procedimiento de solicitud a efectos de:
    a. Información sobre el estado de una solicitud;
    b. Evaluaciones de la autoridad de control competente con respecto a:
        i. reacciones;
        ii. decisiones de la autoridad de control competente.

9.3.2 Documentación de las actividades de evaluación

La autoridad de control podrá establecer requisitos adicionales.

[21] La autoridad de control competente puede especificar y añadir requisitos adicionales si son conformes a la legislación nacional.

9.3.3 Gestión de la tramitación de reclamaciones

La tramitación de reclamaciones será parte integrante del sistema de gestión, que implementará en particular los requisitos establecidos en los puntos 4.1.2.2 letra c), 4.1.2.2 letra j), 4.6 letra d), y 7.13 de la norma ISO/IEC 17065/2012.

Las reclamaciones y objeciones relevantes deben ponerse en conocimiento de la autoridad de control competente.

9.3.4 Gestión de la retirada

Los procedimientos en el caso de suspensión o retirada de la acreditación estarán integrados en el sistema de gestión del organismo de certificación, incluidas las notificaciones a los clientes.