ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD)

aepd agencia española protección datos

ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD)

Redactado por el Área de Certificación de la Agencia Española
de Protección de Datos
23 de diciembre 2019. Versión 1.4

aepd agencia española protección datos

Índice

1. OBJETO 3
1.1 REFERENCIAS 4
1.2 ACRÓNIMOS 4
2 AGENTES DEL ESQUEMA 4
3 MARCA DEL ESQUEMA 5
4 COMITÉ DEL ESQUEMA 5
5 DE LAS ENTIDADES DE CERTIFICACIÓN QUE OPERAN EN EL ESQUEMA 5
5.1 REQUISITOS GENERALES 5
5.2 REQUISITOS ESPECÍFICOS DEL ESQUEMA 6
5.2.1 Relativos a la independencia e imparcialidad 6
5.2.2 Requisitos relativos a la formación y los exámenes 6
5.2.4 Requisitos relativos al proceso de reconocimiento de Entidades de Formación 7
5.2.5 Requisitos relativos al uso de la Marca del Esquema 7
5.3 PROCESO DE EVALUACIÓN 7
5.4 INCUMPLIMIENTO DE LOS REQUISITOS DEL ESQUEMA 9
6 CÓDIGO ÉTICO 9
7 PROCESO DE CERTIFICACIÓN PARA DELEGADOS DE PROTECCIÓN DE DATOS 10
7.1 PERFIL DEL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS 10
7.2 COMPETENCIAS REQUERIDAS AL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS. 12
7.3 PRERREQUISITOS 13
7.4 CÓDIGO ÉTICO 14
7.5 MÉTODO DE EVALUACIÓN 14
7.5.1 Examen 14
7.5.2 Banco de preguntas 16
7.5.3 Programa o Lista de Contenidos 17
7.6 CRITERIOS PARA LA CERTIFICACIÓN 18

7.6.1 Solicitudes y desarrollo del proceso 18
7.6.2 Concesión del certificado. 18
7.6.3 Mantenimiento 19
7.6.4 Renovación de la Certificación 19
7.7 SUSPENSIÓN O RETIRADA DE LA CERTIFICACIÓN 20
7.7.1 Suspensión temporal voluntaria 20
7.7.2 Suspensión temporal por conductas contrarias al Esquema 21
7.7.3 Retirada de la certificación 22
7.8 DERECHOS Y OBLIGACIONES DE LAS PERSONAS CERTIFICADAS 22
7.8.1 Derechos 22
7.8.2 Obligaciones 23
7.8.3 Información sobre personas certificadas 23
8 GESTIÓN DE QUEJAS Y RECLAMACIONES SOBRE EL ESQUEMA 24
8.1 ÁMBITO DE APLICACIÓN 24
8.2 ÓRGANOS COMPETENTES 24
8.3 PROCEDIMIENTO DE QUEJAS Y RECLAMACIONES. 25
9 SEGUIMIENTO Y SUPERVISIÓN DEL ESQUEMA 26
10 DISPOSICIÓN TRANSITORIA 26
ANEXOS 28

1. OBJETO

El objeto de este documento es establecer las condiciones y requisitos que conforman y regulan el funcionamiento del Esquema de Certificación de Personas para la categoría de "Delegado de Protección de Datos" (en adelante, Esquema AEPD – DPD, o el Esquema), recogida en la Sección 4 del capítulo IV 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 las interrelaciones entre los diferentes Agentes que están implicados en dicha certificación bajo condiciones de acreditación.

La certificación de personas es una herramienta adecuada y válida para la evaluación objetiva e imparcial de la competencia de un individuo para realizar una actividad determinada. La ulterior declaración pública hecha por el certificador proporciona al mercado una información útil y contrastada sobre los criterios aplicados y los requisitos exigidos a las personas para obtener la certificación profesional. La validez y vigencia de las reglas del Esquema se asegura a través de la implicación activa de expertos y de representantes de las diferentes partes interesadas en su desarrollo.

La competencia técnica de las entidades de certificación involucradas y su alineamiento con los requisitos fijados por el Esquema, así como su actuación sistemática e imparcial, se consiguen a través de su acreditación por parte de la Entidad Nacional de Acreditación (en adelante, ENAC), de acuerdo con requisitos de normas internacionales para la certificación de personas.

La Agencia Española de la Protección de Datos (en adelante, AEPD, o la Agencia), como propietaria del Esquema, se responsabiliza de su desarrollo y revisión implicando, de forma activa en ambos procesos, a las diferentes partes interesadas a través de un Comité Técnico, sujeto a un Reglamento de funcionamiento, que asegure tanto la representación equitativa de todas las partes implicadas como el encuentro periódico para el análisis y evaluación del trabajo y de las tareas del DPD y de su coherencia con los requisitos de competencia y los mecanismos para su evaluación.

La AEPD define, a través del citado Comité, los criterios para el reconocimiento de las entidades que puedan realizar la evaluación de conformidad (certificación), encaminados a posibilitar la concesión de la "Marca de Conformidad" asociada al Esquema APD - DPD por ella promovido, que identifica de manera exclusiva e inequívoca a aquellas personas que hayan evidenciado su competencia para desempeñar las tareas del DPD.

1.1 REFERENCIAS

- UNE-EN ISO/IEC 17024:2012. Evaluación de Conformidad. Requisitos generales para los organismos que realizan certificación de personas.
- 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, por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

Todos los documentos citados son aplicables en su última edición válida.

1.2 ACRÓNIMOS

- DPD: Delegado de Protección de Datos.
- Esquema AEPD-DPD: Esquema de Certificación de DPD de la AEPD.
- RGPD: Reglamento general de protección de datos.
- LOPDPGDD: Ley Orgánica de protección de datos de personales y garantía de los derechos digitales.

2. AGENTES DEL ESQUEMA

- **La Agencia Española de Protección de Datos (AEPD).** Propietaria del Esquema, es responsable de promover su desarrollo, revisión y validación continua y autoriza al resto de los agentes para formar parte activa del mismo.

- **La Entidad Nacional de Acreditación (ENAC).** Designada por la AEPD como organismo único para la acreditación de las entidades de certificación que deseen participar en el Esquema, teniendo presente tanto los requisitos de la norma UNE-EN ISO/IEC 17024:2012, como los requisitos específicos definidos por el Esquema.

- **Las Entidades de Certificación (EC).** Ofrecen la certificación, exclusivamente bajo acreditación ENAC y de acuerdo con lo requerido por el Esquema y la norma UNE-EN ISO/IEC 17024:2012, para la categoría de "Delegado de Protección de Datos". Como parte del proceso podrán recibir derechos de uso y derechos para licenciar el uso de la "Marca de Conformidad" a las Entidades de Formación y a las personas certificadas, en los términos establecidos en el Anexo II.

3. MARCA DEL ESQUEMA

La AEPD, al objeto de que el mercado identifique a los Delegados de Protección de Datos certificados según el Esquema, ha creado una Marca de Conformidad con el Esquema (en adelante, la Marca del Esquema, o la Marca). La AEPD, mediante contrato, podrá conceder a las Entidades de Certificación los derechos de su uso de la Marca (Anexo II.B).

Podrán hacer uso de la Marca del Esquema las Entidades de Certificación, las Entidades de Formación y los Delegados de Protección de Datos en los términos establecidos en el Anexo II.A.

Las Entidades de Certificación son responsables de velar por el cumplimiento de las normas de uso de marca, tanto por ellas mismas como por las entidades de formación, a las que hayan reconocido sus programas de formación, y por los delegados de protección de datos a los que hayan certificado.

4. COMITÉ DEL ESQUEMA

La AEPD se responsabiliza del desarrollo, revisión y validación del Esquema de certificación de DPD de manera periódica, y al menos cada cinco años, pudiéndose revisar antes si las condiciones de su aplicación así lo aconsejasen. Para ello, ha creado y mantiene un Comité Técnico del Esquema de certificación de DPD (en adelante, el Comité del Esquema, o Comité Técnico), como mecanismo para contactar e involucrar a las distintas partes interesadas en la certificación de personas para el desarrollo de las funciones del Delegado de Protección de Datos. La involucración de las partes interesadas a través del citado Comité será continua en la validación y el mantenimiento del Esquema.

El Comité del Esquema está constituido por la AEPD, como propietaria del mismo, y por las entidades, organizaciones y asociaciones interesadas.

Su organización y régimen de funcionamiento se rige por un Reglamento interno.

5. DE LAS ENTIDADES DE CERTIFICACIÓN QUE OPERAN EN EL ESQUEMA

5.1 REQUISITOS GENERALES

Para poder operar dentro del Esquema, las EC deberán:

- Superar la fase de evaluación para poder ser acreditadas por ENAC, de acuerdo con los requisitos establecidos en la norma UNE-EN ISO/IEC 17024:2012 y en este Esquema
- Haber suscrito y estar vigente el contrato de uso de la Marca (Anexo II.B)

- Cumplir el código de conducta (Anexo III)
- Operar desde una sede en territorio Nacional, que será la que solicite la acreditación

Las decisiones de acreditación de Entidades de Certificación son de la exclusiva competencia de ENAC. La AEPD puede aportar personal técnico para formar parte de los equipos auditores de ENAC en calidad de expertos. Esta participación en ningún caso implica responsabilidad de la AEPD en las decisiones relativas a la acreditación de las EC que son competencia exclusiva de ENAC.

A estos efectos, la AEPD informará a ENAC de cualquier circunstancia de la que tenga conocimiento que pueda suponer un incumplimiento de los requisitos de acreditación, o de las condiciones para operar en el Esquema.

Con el fin de proporcionar transparencia sobre las Entidades de Certificación acreditadas por ENAC, la AEPD publicará en su página web la siguiente información que será facilitada por ENAC: el nombre completo de la entidad acreditada, su página web, la fecha de acreditación y el enlace al anexo técnico de acreditación emitido por ENAC.

5.2 REQUISITOS ESPECÍFICOS DEL ESQUEMA

5.2.1 Relativos a la independencia e imparcialidad

Las Entidades de Certificación y su personal no podrán realizar labores de consultoría, auditoría, o asesoramiento en materia de protección de datos y/o privacidad, directa o indirectamente, que comprometan la independencia e imparcialidad de las EC en las tareas de evaluación y certificación.

Las Entidades de Certificación deberán comunicar a ENAC, de la manera que ésta determine, cualquier circunstancia que pudiera afectar o alterar el cumplimiento de los requisitos de independencia e imparcialidad.

5.2.2 Requisitos relativos a la formación y los exámenes

Preservar la confidencialidad de las preguntas es fundamental para mantener el nivel de exigencia, calidad y fiabilidad que persigue el Esquema. Por ello las entidades de certificación deberán:

- Designar a un responsable que será el único que pueda solicitar los exámenes y que se hará cargo de que las preguntas de los exámenes se custodian en la EC con las debidas medidas de seguridad asegurando que no se produzca ninguna filtración. A estos

efectos, las EC deberán disponer documentalmente de su compromiso de confidencialidad.

- Establecer las medidas técnicas y organizativas necesarias para evitar que los candidatos puedan obtener o copiar las preguntas de los exámenes.

Las EC deben supervisar que los profesionales de los que disponen para la certificación de DPD, en especial los evaluadores, cumplen con estas obligaciones. En caso de detectar alguna anomalía deben proceder a cancelar la relación que les vincule. Las EC deben velar porque estos profesionales de cuyos servicios pueden prescindir no conserven ningún tipo de documentación ni revelen ninguna información sujeta a confidencialidad mediante su compromiso por escrito.

5.2.3 Requisitos relativos a los evaluadores

Las EC son responsables de designar los evaluadores de acuerdo con los requisitos descritos en el citado Anexo VI.

5.2.4 Requisitos relativos al proceso de reconocimiento de Entidades de Formación

Se recogen la parte II del Anexo I

5.2.5 Requisitos relativos al uso de la Marca del Esquema

Las Entidades de Certificación establecerán procedimientos para garantizar que ellas mismas, las Entidades de Formación, cuyos programas de formación hayan reconocido, y los DPD que haya certificado usan la Marca del Esquema conforme a las normas y al contrato de uso, recogidas en el Anexo II.A y B, respectivamente. Estos procedimientos deben asegurar que dichas normas son conocidas por las EF y los DPD certificados, que se han de comprometer contractualmente a respetarlas, y que se ejerce el adecuado control de su uso y se toman medidas en caso de una utilización de la Marca que incumpla lo establecido en dichas normas.

La AEPD podrá en todo momento solicitar información sobre dichos procedimientos.

5.3 PROCESO DE EVALUACIÓN

Las entidades interesadas en operar en el esquema deberán solicitar la acreditación a ENAC para lo que deberán presentar:

- Solicitud de acreditación establecida por ENAC que incluya toda la información que en ella se estipula (disponible en www.enac.es)
- Contrato de uso de marca firmado con la AEPD (Anexo II.B)

- Declaración responsable de que se cumple con el código de conducta establecido en el Anexo III

Recibida dicha documentación, ENAC procederá de conformidad con lo establecido en el Procedimiento de Acreditación y, una vez se haya aceptado la solicitud, informará a la AEPD.

Durante el proceso de evaluación las entidades interesadas deberán:

- Elaborar 300 preguntas de examen que han de ser aprobadas por la AEPD, conforme se dispone en la cláusula 7.5.2.
- Realizar dos convocatorias de examen, una vez dispongan de la aprobación de las preguntas por la AEPD, con un mínimo de 5 y un máximo de 15 candidatos en cada una que cumplan todos los prerrequisitos exigidos en el Esquema.

  La entidad interesada deberá informar a los candidatos que examinen en la fase de evaluación de que se trata de un examen condicionado a la obtención de la acreditación, por lo que aquellos que hayan superado la prueba obtendrán su certificado sólo cuando la entidad haya sido acreditada y siempre que, en la auditoria previa a la obtención de la acreditación, no se hubieran detectado irregularidades que afecten a cualquiera de las fases de que consta el proceso de examen.

Así mismo, las entidades interesadas podrán reconocer únicamente un programa de formación, debiendo informar a las EF de que dicho reconocimiento está sujeto a la obtención de su acreditación como Entidad de Certificación. No se podrá dar comienzo a la formación hasta que no se obtenga la acreditación por ENAC.

Las entidades interesadas no podrán ofrecer ni publicitar servicios relacionados con el Esquema AEPD-DPD hasta que no dispongan de la acreditación de ENAC.

Transcurridos seis meses desde la presentación de la solicitud de acreditación sin que las entidades interesadas la hayan obtenido por razones imputables a ellas, aquélla quedará sin efecto de manera automática, sin perjuicio de la resolución del contrato de uso de la Marca (véase cláusula 5.4 y Anexo II.B).

Cuando la AEPD tenga conocimiento del incumplimiento por parte de una entidad interesada en obtener la acreditación de ENAC de las condiciones del Esquema, incluidos los compromisos del código ético, se comunicará a ENAC que actuará de acuerdo con el Procedimiento de Acreditación. Sin perjuicio de lo anterior, en estos casos, la AEPD, motivadamente y previa audiencia de la otra parte, podrá resolver el contrato de uso de Marca.

5.4 INCUMPLIMIENTO DE LOS REQUISITOS DEL ESQUEMA

ENAC actuará de acuerdo con lo establecido en el Procedimiento de Acreditación en caso de incumplimiento de los requisitos de acreditación que se pongan de manifiesto en las auditorías de seguimiento, o de cualquier otra forma y momento.

ENAC informará inmediatamente a la AEPD de la suspensión o retirada de las acreditaciones concedidas, así como de los motivos que la justifican, que pueden dar lugar a la resolución del contrato de uso de la Marca.

La resolución del contrato de uso de la Marca, sin perjuicio de las actuaciones que por parte de ENAC procedan con arreglo al Procedimiento de Acreditación, implicará que la entidad afectada no podrá ofrecer servicios de certificación dentro del Esquema AEPD – DPD y, en consecuencia, la extinción automática de la acreditación.

La AEPD no suscribirá contratos de uso de la Marca con entidades cuya acreditación se haya retirado por ENAC, o se haya extinguido hasta transcurridos 2 años desde la fecha de la retirada o la extinción.

En caso de retirada o extinción de la acreditación, las entidades afectadas:

- Deberán informar de dicha situación de manera inmediata a los DPD a los que haya certificado con arreglo al Esquema, a fin de que se dirijan a otra EC para que se les reconozca su certificación y les permita renovarla según se establece en el Esquema, sin que se les exija ningún requisito adicional.

  Las EC a las que se dirijan los DPD asumirán las obligaciones correspondientes a la concesión de la certificación del Esquema.

- Deberán informar de dicha situación de manera inmediata a las EF cuyos programas de formación hubieran reconocidos, a fin de que se dirijan a otra EC para su reconocimiento. Las EF deberán solicitar el reconocimiento siguiendo el procedimiento establecido en la EC a la que se dirijan.

6. CÓDIGO ÉTICO

A efectos de justificar cuestiones como la integridad y un elevado nivel de compromiso ético por parte de las entidades interesadas en acreditarse como entidades de certificación bajo el Esquema AEPD-DPD, las acreditadas y las entidades que ofrecen programas de formación bajo el Esquema han de observar los principios, valores y compromisos que se recogen en el Código Ético que forma parte del Esquema como Anexo III.

El Código Ético debe ser aceptado por las entidades interesadas en obtener la acreditación en el momento de solicitarla.

El Código Ético debe ser aceptado por las entidades interesadas en obtener el reconocimiento de sus programas de formación junto con la solicitud de dicho reconocimiento.

Las EC y las EF han de dar visibilidad a sus compromisos éticos mediante la publicación del Código Ético en su página web.

El incumplimiento del código ético podrá ser causa de resolución del contrato de uso de la Marca (véase cláusula 5.4 y Anexo III).

ENAC informará de manera inmediata a la AEPD de cualquier circunstancia de la que tenga conocimiento que pueda suponer un incumplimiento del Código Ético.

7. PROCESO DE CERTIFICACIÓN PARA DELEGADOS DE PROTECCIÓN DE DATOS

El Esquema establece los requisitos de competencia para la persona que desempeñe el puesto de Delegado de Protección de Datos, así como los criterios para evaluar su posesión por parte de las personas aspirantes, de manera que, cuando el resultado de tal proceso de evaluación sea favorable, la entidad de certificación emitirá una declaración de cumplimiento o certificado.

7.1 PERFIL DEL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS

El DPD es un profesional cuyas funciones se recogen en el artículo 39 del RGPD y en los artículos 36 y 37 de la LOPDPGDD, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos**.**

El DPD tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable, o al encargado del tratamiento, y a las personas autorizadas para tratar los datos personales bajo su autoridad directa, en virtud del RGPD, la LOPDPGDD y de otras disposiciones de protección de datos de la UE o de sus Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el RGPD, la LOPDPGDD y en otras disposiciones de protección de datos de la UE o de sus Estados miembros, y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales;
c) supervisar la asignación de responsabilidades;
d) supervisar la concienciación y formación del personal que participa en las operaciones de tratamiento;

e) supervisar las auditorías correspondientes;
f) ofrecer el asesoramiento que se le solicite acerca de las evaluaciones de impacto relativas a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD;
g) cooperar y actuar como interlocutor con la autoridad de control para las cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a que se refiere el artículo 36 del RGPD.

El DPD desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Para ello deberá ser capaz de:

a) recabar la información necesaria para determinar las actividades de tratamiento;
b) analizar y comprobar la conformidad de las actividades de tratamiento con la normativa aplicable;
c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento;
d) recabar información para supervisar el registro de las operaciones de tratamiento;
e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto;
f) asesorar sobre:
   - si se debe llevar a cabo o no una evaluación de impacto de la protección de datos y en qué áreas o tratamientos,
   - qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos,
   - si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o mediante contratación externa,
   - qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados,
   - si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos y
   - si sus conclusiones (seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el RGPD;
g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos;
h) asesorar sobre qué actividades de formación internas proporcionar al personal y a los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos;
i) intervenir en caso de reclamación ante las autoridades de protección de datos.

7.2 COMPETENCIAS REQUERIDAS AL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS

El DPD deberá reunir conocimientos especializados del Derecho y la práctica en materia de protección de datos. Se han identificado, en consecuencia, aquellos conocimientos, habilidades y destrezas necesarias que tiene que poseer la persona a certificar para llevar a cabo cada una de las funciones propias de la posición de Delegado de Protección de Datos.

Las funciones genéricas del DPD se pueden concretar en tareas de asesoramiento y supervisión, entre otras, en las siguientes áreas:

1. Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
2. Identificación de las bases jurídicas de los tratamientos.
3. Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
4. Determinación de la existencia de normativa sectorial que pueda estipular condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
5. Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
6. Establecimiento de procedimientos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
7. Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
8. Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
9. Identificación de los instrumentos para las transferencias internacionales de datos adecuados a las necesidades y características de la organización, y de las razones que justifiquen la transferencia.
10. Diseño e implantación de políticas de protección de datos.
11. Auditoría de protección de datos.
12. Establecimiento y gestión de los registros de actividades de tratamiento.
13. Análisis de riesgos de los tratamientos realizados.
14. Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
15. Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
16. Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
17. Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.

18. Realización de evaluaciones de impacto sobre la protección de datos.
19. Relaciones con las autoridades de supervisión.
20. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

7.3 PRERREQUISITOS

Para acceder a la fase de evaluación será necesario el cumplimiento de alguno de los siguientes prerrequisitos:

1) Justificar una experiencia profesional de, al menos, cinco años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD.

2) Justificar una experiencia profesional de, al menos, tres años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD, y una formación mínima reconocida de 60 horas en relación con las materias incluidas en el programa del Esquema.

3) Justificar una experiencia profesional de, al menos, dos años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD, y una formación mínima reconocida de 100 horas en relación con las materias incluidas en el programa del Esquema.

4) Justificar una formación mínima reconocida de 180 horas en relación con las materias incluidas en el programa del Esquema.

Las condiciones para la justificación de los prerrequisitos se detallan en el Anexo I del presente Esquema.

A estos efectos, se computarán igual las horas de formación, ya sean online o presenciales, siempre que se cumplan el resto de los requisitos de formación establecidos en el Esquema.

Se valorará toda la experiencia adquirida, tanto anterior como posterior a la publicación del RGPD (BOE del 4 de mayo de 2016) y realizada en el ámbito nacional y de la Unión Europea.

Las entidades de formación solicitarán a las de certificación el reconocimiento de los programas de formación que imparten de acuerdo con los criterios y el procedimiento establecidos en la parte II del Anexo I.

En caso de no cumplir con la experiencia requerida se podrá convalidar hasta un año de experiencia mediante la justificación de méritos adicionales.

7.4 CÓDIGO ÉTICO

A los efectos de justificar cuestiones como la integridad y el elevado nivel de ética profesional que implica la función de DPD, se ha elaborado, y forma parte del Esquema, un código ético con principios, valores y compromisos que ha de ser aceptado por los candidatos a obtener la certificación con carácter previo a su concesión. El código ético se recoge en el Anexo IV.

7.5 MÉTODO DE EVALUACIÓN

El proceso de evaluación está basado tanto en la valoración del conocimiento y experiencia como en el desarrollo profesional continuo.

A través de las correspondientes pruebas de evaluación, el candidato deberá evidenciar que posee la competencia adecuada, es decir, los conocimientos teóricos, la capacidad profesional y las habilidades personales necesarias para llevar a cabo las funciones correspondientes a la actividad de Delegado de Protección de Datos, en los términos y condiciones establecidos por el Esquema de certificación de la AEPD.

7.5.1 Examen

La evaluación de los conocimientos y capacidades técnicas o profesionales se llevará a cabo mediante la realización de un examen, con las siguientes características:

- El examen versará sobre los temas relativos a los conocimientos específicos indicados en el programa del Esquema, detallado en el apartado 6.5.3, de conformidad con los criterios de ponderación establecidos para cada uno de los dominios en que se estructuran los correspondientes conocimientos y competencias a evaluar.
- Es requisito imprescindible para la obtención del certificado la superación del examen. El objetivo del examen es evaluar los conocimientos teórico-prácticos de un candidato para realizar las funciones de Delegado de Protección de Datos.
- El examen consiste en contestar 150 preguntas tipo test de respuesta múltiple. El 20% de las preguntas, es decir, 30 preguntas, describirán un escenario práctico (de carácter normativo, organizativo y/o técnico) sobre el que versará la pregunta.
- Las preguntas están distribuidas en cada uno de los correspondientes bloques o dominios del programa conforme a la siguiente ponderación:
    - Dominio 1 – 50%, 75 preguntas, de ellas 15 con escenario práctico.
    - Dominio 2 – 30%, 45 preguntas, de ellas 9 con escenario práctico.
    - Dominio 3 – 20%, 30 preguntas, de ellas 6 con escenario práctico.

- Para la aprobación de la prueba se requiere haber respondido correctamente el 75% (al menos 113 puntos), de la siguiente forma: un 50% de respuestas correctas en cada uno de los bloques o dominios. Es decir, deberán obtenerse 75 puntos sumando la puntuación mínima de los tres dominios, y el resto de la puntuación hasta obtener el 75% del total se podrá obtener de cualquiera de los dominios.

- Las preguntas tendrán cuatro opciones de respuesta, de las cuales solo una será válida. Cada respuesta correcta contará como 1 punto. No se puntúan las preguntas cuya respuesta sea incorrecta o se deje en blanco.

- La duración del examen es de cuatro horas.

- El resultado de la prueba de evaluación comportará la valoración de "apto" o "no apto" en cada convocatoria.

- Cada entidad de certificación llevará a cabo las convocatorias que estime oportunas, y deberá comunicar su fecha de celebración a la AEPD con una antelación de al menos 1 mes.

Mediante acuerdo de todas las entidades de certificación, se puedan establecer convocatorias únicas y coordinadas.

Las tareas de supervisión y corrección de exámenes pueden ser realizadas por personal administrativo de las EC siempre y cuando esté sujetos al deber de confidencialidad mediante compromiso que conste por escrito.

- Si no se producen alegaciones durante el proceso de examen por parte de los candidatos, la corrección pasará directamente al proceso de dictamen sin necesidad de revisión por parte del evaluador.
- Si en el proceso de examen se produce alguna alegación, ésta debe ser valorada previamente por el evaluador que será quién dictamine sobre la misma, firmando el informe correspondiente.

El proceso de corrección, así como, en su caso, el de gestión de alegaciones por parte del evaluador debe ser anónimo para la persona que corrige y para el evaluador.

El evaluador ha de garantizar la independencia de criterio, mediante la emisión de un registro con el resultado de la evaluación del candidato en el cual se basa la decisión de concesión del certificado.

Las EC deben informar a los candidatos del resultado del examen y para ello utilizarán el modelo de informe que se recoge en el Anexo VII.

No está permitido facilitar o mostrar los exámenes a los candidatos que lo soliciten.

7.5.2 Banco de preguntas

La AEPD dispone de un banco de preguntas que se nutre de las aportaciones de todas las entidades acreditadas por ENAC, y, según las necesidades que pueda presentar el banco, requerirá a las EC aportaciones anuales de preguntas que cubran aquellas materias no tratadas, o escasamente tratadas en las preguntas disponibles, en el banco de preguntas, o las novedades legislativas o tecnológicas que se vayan produciendo, priorizando preguntas sobre dominios deficitarios.

Las EC no podrán proporcionar preguntas de examen a las EF ni aceptar de las EF preguntas para aumentar el banco de preguntas de la AEPD.

Las entidades interesadas, para poder ser acreditadas por ENAC, deben elaborar 300 preguntas siguiendo los criterios establecidos por la AEPD, en el documento que les será remitido cuando ENAC le comunique que la solicitud de la entidad ha sido admitida y está en proceso de evaluación para ser acreditada. Este documento es confidencial, por lo que sólo se facilitará a las personas encargadas de la elaboración de las preguntas que deberán comprometerse por escrito a guardar dicho carácter del documento.

Se prohíbe expresamente a las personas que tienen acceso al documento donde se recogen los requisitos exigidos para redactar las preguntas su utilización con cualquier otra finalidad, así como, sobre sus criterios, elaborar y comercializar modelos de preguntas.

La AEPD realizará dos revisiones de las preguntas y si no se ajustasen a los criterios establecidos comunicará a las entidades interesadas las deficiencias observadas. Si después de la segunda revisión las preguntas continuasen sin ajustarse a los criterios establecidos para poder ser aprobadas se tendrá por incumplido este requisito, y no podrá procederse a la realización de los exámenes. Si las 300 preguntas son validadas por la AEPD, la entidad en proceso de evaluación para la obtención de la acreditación por parte de ENAC podrá convocar los exámenes utilizando las citadas preguntas.

Las entidades que se encuentren en proceso de evaluación para la obtención de la acreditación por ENAC, así como las EC deben comunicar a la AEPD las fechas en que tienen previsto celebrar exámenes con una antelación mínima de un mes. En concreto deben facilitar información sobre el día, hora y el lugar en que se va a celebrar el examen (centro, calle, número y ciudad).

La AEPD elaborará el examen utilizando el banco de preguntas y lo enviará, por el sistema establecido en la AEPD, a la Entidad de Certificación para su revisión. Una vez revisado, la AEPD remitirá a la Entidad de Certificación un fichero cifrado conteniendo dos versiones del examen para que se puedan alternar entre los candidatos, así como las plantillas de corrección y un formulario de estadísticas que deben retornar a la AEPD una vez corregidos los exámenes.

La AEPD podrá fijar el formato en que deberán ser aportadas las preguntas, así como los requisitos técnicos y procedimentales para asegurar la calidad y confidencialidad en su entrega.

Para ello pone a disposición un sistema seguro para el intercambio de documentos. No se podrá remitir preguntas o exámenes a la AEPD por un medio distinto de este sistema.

No se permite la comercialización de las preguntas del examen a las que han tenido acceso las EC en el ejercicio de sus funciones certificadoras, así como elaborar preguntas modelo siguiendo los criterios de la AEPD con idéntico fin, lo que incluye la publicación de catálogos con baterías de preguntas.

La AEPD podrá elaborar un juego de preguntas modelo que será de pública disposición.

7.5.3 Programa o Lista de Contenidos

Los contenidos a evaluar en el examen de la certificación están integrados en los siguientes dominios o áreas temáticas según las ponderaciones indicadas:

Dominio 1 NORMATIVA GENERAL DE PROTECCIÓN DE DATOS. Cumplimiento normativo del reglamento europeo, normativa nacional, directiva europea sobre ePrivacy. Directrices y guías del Comité Europeo de Protección de Datos, etc.

Ponderación: 50%.

Dominio 2 RESPONSABILIDAD ACTIVA. Evaluación y gestión de riesgos de los tratamientos de datos personales, evaluación de impacto de protección de datos, protección de datos desde el diseño, protección de datos por defecto, etc.

Ponderación: 30%.

Dominio 3 TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS Y OTROS CONOCIMIENTOS. Auditorías de seguridad, auditorías de protección de datos, etc.

Ponderación: 20%.

Los contenidos del temario están especificados en el Anexo V.

7.6 CRITERIOS PARA LA CERTIFICACIÓN

7.6.1 Solicitudes y desarrollo del proceso

Quienes deseen obtener la certificación como DPD deberán cumplir con los prerrequisitos establecidos en el apartado 6.3 y presentar la siguiente documentación ante cualquiera de las EC:

a) Formulario de solicitud
b) Currículum detallado
c) Documentación justificativa del cumplimiento de los prerrequisitos
d) Justificación del abono de la tasa correspondiente

A través de dicha solicitud el candidato declara conocer el proceso de certificación descrito en este documento y acepta participar en las pruebas de evaluación.

Una vez presentada la solicitud, la EC procederá a verificar si la documentación está completa y justifica los requisitos exigidos.

Si la documentación no estuviera completa se informará por escrito al candidato de las deficiencias advertidas, y se le concederá un plazo de 10 días hábiles para su subsanación. Transcurrido dicho plazo sin que se hubiera procedido a la subsanación se declarará al candidato como no admitido, lo que igualmente se le comunicará por escrito.

Si la solicitud es aceptada se informará por escrito al candidato, de la misma manera se procederá si la admisión fuese para una convocatoria distinta de la solicitada en caso de existir varias.

Cualesquiera decisiones de la EC respecto al proceso de aceptación podrán ser objeto de la correspondiente reclamación en los términos establecidos en el apartado 8 del presente Esquema.

Por convocatoria se entiende el anuncio de la realización de las pruebas de evaluación por una EC, en una fecha y centro de examen determinados.

Para acceder al examen los solicitantes deberán presentar documentación que acredite su identidad.

Los candidatos que no superen la prueba de evaluación serán informados, previamente a la realización del nuevo examen en el caso de que tengan derecho a una segunda prueba, de su resultado por escrito, conforme al modelo que se recoge en el Anexo VII.

7.6.2 Concesión del certificado

Las EC concederán la certificación a los candidatos que hubieran obtenido el resultado de “apto”, y les emitirá un certificado justificativo, conforme al modelo que se recoge en el Anexo VIII, que se enviará a cada uno de ellos.

Para la emisión de la certificación será requisito previo que el candidato se comprometa expresamente a observar el Código Ético y las normas de uso de la Marca del certificado.

Las EC asignarán a cada DPD que hayan certificado un número personal intransferible que será utilizado en el futuro para su identificación, junto con el número identificativo de la entidad de certificación que emitió el certificado.

El certificado emitido tendrá un período de validez de tres años, salvo sanción de suspensión o retirada de la certificación. El período de validez comenzará a partir de la fecha de concesión del certificado.

7.6.3 Mantenimiento

En el caso de que durante el período de validez del certificado se produjesen cambios legales, o tecnológicos que, a juicio del Comité del Esquema, hiciesen conveniente una revisión o adaptación significativa del certificado concedido, se podrán establecer los criterios adecuados para mantener la vigencia de los certificados ya concedidos.

7.6.4 Renovación de la Certificación

La renovación del certificado requerirá que el candidato justifique haber cumplimentado:

- un mínimo de 60 horas de formación recibida y/o impartida durante el periodo de validez del certificado, requiriéndose un mínimo anual de 15 horas en materias objeto del programa del Esquema, y,
- al menos, un año de experiencia profesional en proyectos y/o actividades y tareas relacionadas con las funciones del DPD y/o de la seguridad de la información, evidenciada por tercera parte (empleador o similar).

Se valorará la formación impartida con el doble de horas que la formación recibida.

Para que la formación recibida se considere válida debe proporcionar una actualización demostrable de los conocimientos objeto del Esquema y sólo se tendrá en cuenta la formación recibida durante el período de vigencia de la certificación. No será válida la formación reconocida para presentarse al examen de certificación.

Para que el certificado de formación sea valorado debe constar la entidad de formación que lo imparte y el título de la formación, fecha y número de horas, temario y formato (presencial u online). En el caso de no poder justificar la formación anual mínima requerida durante alguno de los tres años exigidos, se permite la cumplimentación de esa formación en alguno de los otros dos años restantes. Se considera formación la asistencia a seminarios y congresos siempre que el candidato aporte certificado con la misma información solicitada para un programa de formación.

La EC notificará a la persona certificada el final del período de validez de la certificación con una antelación mínima de tres meses.

La renovación habrá de solicitarse con anterioridad a la fecha de vencimiento del periodo de validez del certificado. La no recepción por la persona certificada de la comunicación de la EC informando del final del periodo de validez de la certificación, no eximirá del cumplimiento de lo indicado en este apartado.

El candidato deberá presentar la solicitud de renovación a cualquiera de las EC junto con la relación de las reclamaciones que, en su caso, le hayan presentado durante el período completo de validez de la certificación por actuaciones deficientes en la actividad propia para la que esté certificado, o bien una declaración en la que haga constar que no ha sido objeto de ninguna reclamación. Deberá acompañar la aceptación del Código Ético y de las normas de uso de la Marca del certificado, además de la justificación del pago de las tasas de renovación.

La Entidad de Certificación procederá a la valoración de la solicitud y de la documentación aportada. Si como resultado de la valoración se concluyese que no se reúnen los requisitos para la renovación de la certificación, se comunicará por escrito al interesado las deficiencias advertidas y se le concederá un plazo de 90 días naturales para que proceda a subsanarlas. Transcurrido dicho plazo sin que se hubiera procedido a su subsanación se declarará al candidato como no renovado, lo que se le comunicará por escrito y se procederá a la retirada del certificado.

Si la solicitud es aceptada, igualmente se informará por escrito al interesado.

La renovación de la certificación implicará un nuevo certificado justificativo a emitir por la EC con el mismo número personal asignado en la primera certificación. El nuevo certificado tendrá un periodo de validez de tres años.

7.7 SUSPENSIÓN O RETIRADA DE LA CERTIFICACIÓN

7.7.1 Suspensión temporal voluntaria

En el caso en que la persona certificada declare haber dejado de cumplir los requisitos del Esquema, contractuales o de otro orden, su certificación dejará de estar en vigor durante un tiempo no superior a 12 meses.

Para la reactivación de su vigencia, la entidad de certificación realizará las comprobaciones oportunas encaminadas a verificar que las causas que motivaron la solicitud de suspensión han desaparecido, siempre que no haya transcurrido más de un año desde la fecha de suspensión de la certificación y se justifique documentalmente que se está en condiciones de obtener el certificado, en los términos establecidos para su renovación en el apartado anterior.

Una vez transcurrido un año de suspensión del certificado, sin que haya sido posible la reactivación de su vigencia, o no hayan desaparecido las causas que motivaron la suspensión, se procederá a la retirada definitiva de la certificación y el interesado deberá, en su caso, reiniciar todo el proceso para obtener nuevamente la misma.

7.7.2 Suspensión temporal por conductas contrarias al Esquema

Son motivos de suspensión de la certificación por la entidad de certificación los siguientes:

- La no presentación por parte de la persona certificada de la documentación, registros o de cualquier información que le haya sido requerida al DPD por la entidad de certificación para mantenerla, o para investigar una reclamación contra su actuación.

- La no realización de alguna de las funciones y tareas como DPD, así como la falta o ausencia de competencia para cualquier tarea asignada bajo este Esquema.

- La realización por parte de la persona de declaraciones o usos en su condición de certificado que excedan del alcance de la certificación, que sean engañosas o que de cualquier manera perjudiquen o desprestigien el Esquema de certificación.

- Los comportamientos contrarios al Código Ético.

- El uso de la Marca del Esquema de manera no permitida o contraria a las reglas de su uso.

- El incumplimiento por la persona certificada de cualquiera otra de las reglas del Esquema que le afecten.

Cualquiera de estos incumplimientos podrá dar lugar a la suspensión temporal de la certificación por un período máximo de seis meses. La acumulación de tres incumplimientos podrá suponer la suspensión de la certificación por un periodo entre seis meses y la mitad del ciclo de vigencia de la certificación, que en caso de superar el plazo de vigencia se procederá a su retirada.

Si, como consecuencia de la investigación de estos supuestos, la entidad de certificación concluye que existen evidencias de que el DPD ha dejado de cumplir con los requisitos del Esquema, contractuales, o de otra orden incluida la posesión de una determinada competencia, y en consecuencia su certificado deje de ser válido, la EC deberá proceder a suspender temporalmente tal certificado en tanto no se subsanen las causas que lo motivan.

Las sanciones establecidas se entenderán sin perjuicio de las responsabilidades civiles, penales, profesionales o de otro orden en que puedan incurrir los DPD certificados en el ejercicio de su profesión.

Para la reactivación del certificado, la EC realizará las oportunas comprobaciones para verificar que las causas que motivaron la suspensión han desaparecido, pudiéndose llegar incluso a exigirse una reevaluación parcial o total.

7.7.3 Retirada de la certificación

Son motivos de retirada de una certificación ya emitida, los siguientes:

- Cualquiera de los identificados anteriormente para la suspensión temporal, en función de su gravedad o su reiteración, como la reiteración en un tipo concreto de incumplimiento que hubiera dado lugar a una suspensión temporal, que implique que no se ha corregido la conducta del DPD.
- La acumulación de más de tres sanciones de suspensión de la certificación.
- La falta de colaboración de la persona certificada para la devolución del certificado en caso de sanción.

Los interesados a los que las EC les haya retirado la certificación y deseen obtenerla de nuevo deberán someterse a un proceso de certificación inicial completo. Las EC podrán requerir a estas personas para que, previamente a someterse a la evaluación, evidencien haber subsanado las causas que llevaron a la retirada del certificado anterior sin que ello pueda ser considerado como trato discriminatorio.

Las EC se reservarán el derecho a aceptar una nueva solicitud por parte del profesional sancionado.

7.8 DERECHOS Y OBLIGACIONES DE LAS PERSONAS CERTIFICADAS

7.8.1 Derechos

Los titulares de los certificados tendrán derecho a:

- Hacer uso de los certificados para el desarrollo de su actividad profesional.
- Beneficiarse de cuantas actividades de divulgación y promoción lleve a cabo la entidad de certificación referente a las personas certificadas.
- Hacer uso de la Marca del Esquema conforme a lo establecido en el Anexo II.
- Reclamar y a recurrir cualquier decisión desfavorable.

7.8.2 Obligaciones

Los titulares de los certificados estarán obligados a:

- Respetar el Esquema de Certificación de DPD y todos los procedimientos aplicables.
- Cumplir con las obligaciones económicas derivadas de la certificación.
- Aceptar las prescripciones del Código Ético.
- Actuar en su ámbito profesional con la debida competencia técnica, velando por el mantenimiento del prestigio de la certificación concedida.
- Colaborar con la entidad de certificación en las actividades de supervisión de su actuación necesarias para el mantenimiento y renovación de la certificación.
- Informar a la entidad de certificación sobre cualquier situación profesional que pudiera afectar al alcance de la certificación concedida.
- Informar a la entidad de certificación, sin demora, sobre cuestiones que puedan afectarle para continuar cumpliendo los requisitos de certificación.
- No usar el certificado del Esquema para fines diferentes que no sean los derivados de la realización de actividades dentro del alcance de la certificación concedida.
- No realizar acciones lesivas, de cualquier naturaleza, ni dañar la imagen y/o los intereses de las personas, empresas, entidades y clientes, incluso potenciales, interesados en la prestación profesional, ni tampoco la de la AEPD o de las entidades de certificación.
- No tomar parte en prácticas fraudulentas relativas a la sustracción y/o divulgación del material de examen.
- Mantener un registro de reclamaciones recibidas en relación con el alcance de la certificación obtenida.
- Devolver el certificado en caso de retirada de la certificación.

El incumplimiento de las obligaciones descritas supondrá el inicio del proceso de suspensión o retirada del certificado.

7.8.3 Información sobre personas certificadas

Las EC mantendrán un registro actualizado de las personas certificadas que incluirá: nombre y apellidos, número de certificado, fecha de concesión, fecha de caducidad y estado del certificado (concedido, suspendido, retirado, renovado).

Las EC publicarán en su web la información contenida en dicho registro, y la comunicarán a la AEPD por el mecanismo que ésta designe. Así mismo, la AEPD publicará en su web dicha información y la de la entidad que ha emitido la certificación.

Las EC son las responsables de mantener actualizada dicha información.

8. GESTIÓN DE QUEJAS Y RECLAMACIONES SOBRE EL ESQUEMA

8.1 ÁMBITO DE APLICACIÓN

Podrán ser objeto de queja o reclamación cualesquiera actuaciones contrarias al Esquema, incluido el Código Ético, realizadas por las entidades de certificación, las entidades de formación y por los Delegados de Protección de Datos certificados.

Serán objeto de especial atención las conductas de los Delegados de Protección de Datos certificados que resulten contrarias al Código Ético que se adjunta como Anexo IV**,** así como las conductas de las entidades citadas que resulten contrarias al Código Ético que se adjunta como Anexo III.

8.2 ÓRGANOS COMPETENTES

Son órganos competentes para conocer y, en su caso, resolver las quejas o reclamaciones que se presenten sobre el Esquema, y por este orden:

- Las Entidades de Certificación (EC)
- La Entidad Nacional de Acreditación (ENAC)
- La Agencia Española de Protección de Datos (AEPD)

Cualquier queja o reclamación sobre la actuación de uno de los Agentes del Esquema deberá ser presentada, en primer lugar, ante el Agente que la haya realizado.

a) Si la reclamación o queja es relativa a un programa de formación reconocido por una EC deberá ser gestionada por ésta de acuerdo con lo requerido por la norma UNE-EN ISO/IEC 17024.
b) Si la reclamación o queja es relativa a la actuación de la EC deberá ser gestionada por ésta de acuerdo con lo requerido por la norma UNE-EN ISO/IEC 17024.
c) Si la reclamación o queja presentada por parte un tercero, bien ante la AEPD, ENAC o una EC, se refiere a la actuación o desempeño de un DPD certificado en el Esquema deberá ser reenviada al resto de agentes y tramitada en primera instancia por la EC que haya certificado al DPD. Las responsabilidades dependerán del contenido de dicha reclamación.
d) Si la reclamación o queja está relacionada con la acreditación concedida deberá ser tramitada por ENAC que, además, deberá tramitar las que procedan de reclamantes insatisfechos con la respuesta dada, en primera instancia, por una EC acreditada.
e) Si la reclamación o queja hace referencia al incumplimiento del Código Ético (Anexo III) por una EF o una EC se deberá plantear ante la entidad reclamada que deberá

comunicarla, junto con la respuesta facilitada, a la EC, en el caso de que se haya dirigido contra una EF y, en todo caso, a la AEPD.

El tratamiento dado a las reclamaciones y quejas, así como su resolución, será verificado por ENAC como parte de su evaluación.

La AEPD sólo podrá intervenir en la gestión y tratamiento de cualquier reclamación o queja recibida en relación con el funcionamiento del Esquema si, previamente, ha sido tramitada por los demás Agentes del Esquema.

Cualquier reclamación que se dirija a la AEPD acerca del Esquema deberá ser comunicada formalmente por escrito, identificando que se trata de una reclamación o queja, y que previamente se ha intentado su resolución ante el Agente del Esquema correspondiente (EC o ENAC, o los dos). La AEPD adoptará la resolución correspondiente que notificará al reclamante.

8.3 PROCEDIMIENTO DE QUEJAS Y RECLAMACIONES

El proceso para el tratamiento y resolución de las quejas o reclamaciones será el establecido por la correspondiente EC conforme a la norma UNE-EN ISO/IEC 17024, que deberá estar disponible al público.

El procedimiento para la gestión de las quejas o reclamaciones sobre el Esquema deberá seguir, al menos, los siguientes trámites:

a) Estudio y valoración de la queja o apelación y, en su caso, petición de evidencias.
b) Comunicación a las partes interesadas y/o afectadas por cada proceso de apelación y reclamación sobre la situación puesta de manifiesto, incluyendo un plazo máximo de 30 días para la presentación de alegaciones.
c) Análisis y evaluación de las evidencias aportadas y las alegaciones presentadas por las partes interesadas.
d) Deliberación y toma de decisión final al respecto.
e) Comunicación de la resolución a las partes.

Para el adecuado desarrollo del presente procedimiento, la persona certificada está obligada a:

a) Colaborar plenamente con cualquier investigación formal abierta para resolver casos específicos de reclamaciones y/o quejas.
b) Mantener un registro de todas las reclamaciones presentadas contra ella por la actividad desarrollada en el ámbito de validez de la certificación, y permitir a la EC el acceso a estos registros. A tales efectos, en el plazo de diez días desde la recepción

de la reclamación, deberá comunicarla por escrito, junto con una copia de la reclamación, a la EC.

c) Proporcionar a los clientes un formulario para formalizar cualquier queja relacionada con los servicios prestados, que se remitirá tanto a la persona certificada y entidad afectada por la queja, así como a la Entidad de Certificación.

Si la queja o reclamación diera lugar a la apertura de una actividad de investigación sobre una persona certificada, cuya resolución pudiera implicar la suspensión temporal o la retirada o pérdida de la certificación obtenida, se estará a lo dispuesto en el apartado 6.7 del presente Esquema.

9. SEGUIMIENTO Y SUPERVISIÓN DEL ESQUEMA

A efectos de garantizar los necesarios estándares de calidad y rigor en el cumplimiento del Esquema por los correspondientes Agentes, se constituye un Comité de Seguimiento integrado por miembros de la Agencia Española de Protección de Datos y de la Entidad Nacional de Acreditación para realizar el seguimiento y control de su funcionamiento.

Adicionalmente, ENAC y la AEPD compartirán información relativa al funcionamiento del Esquema en sus respectivos ámbitos de actuación para garantizar que el Esquema funciona de manera coherente y es consistente con los máximos niveles de exigencia.

10. DISPOSICIÓN TRANSITORIA

El presente Esquema será de aplicación a las entidades interesadas en obtener la acreditación, a las entidades de certificación, a las entidades de formación y a los delegados de protección de datos a partir del día siguiente de su publicación en la página web de la AEPD, quedando extinguidas desde dicho momento las designaciones provisionales que se hubiesen emitido.

Para las entidades interesadas que a la publicación de esta versión ya tuviesen aceptada la documentación en ENAC o se les hubiese emitido la designación provisional, el plazo para acreditarse se mantiene en los 12 meses desde la fecha en que se formalizó la solicitud, debiendo, no obstante, cumplir con los requisitos del presente Esquema para ser acreditada, que se verificarán a través del procedimiento establecido en el mismo. A estos efectos, en el plazo de 1 mes desde la publicación del presente Esquema, deberá suscribirse y remitirse a ENAC el contrato de uso de la Marca del Esquema conforme al modelo del Anexo II.B. y la declaración responsable en la que declare cumplir con el código ético establecido en el Anexo III. La falta de suscripción del contrato o de la declaración responsable determinará la imposibilidad de continuar con el procedimiento de acreditación.

Las entidades acreditadas, en el plazo de 1 mes desde la publicación del presente Esquema, deberán suscribir un nuevo contrato de uso de la Marca adaptado al modelo del Anexo II.B. y la declaración responsable en la que declare cumplir con el código ético establecido en el Anexo III. La falta de suscripción del contrato o de la declaración responsable determinará la resolución del contrato en vigor y la extinción de la condición de Agente del Esquema.

Asimismo, las entidades acreditadas tienen un plazo de 3 meses desde la publicación del presente Esquema para sustituir los certificados emitidos a los DPD certificados por unos nuevos que incorporen el logo actualizado. Además, deberán comunicar a las EF con programas reconocidos que en ese plazo han de cambiar el logo en sus páginas web y actualizar la suya.

Las EC tienen un plazo de 1 mes, desde la publicación del presente Esquema, para requerir a las EF a las que haya reconocido sus programas que firmen la declaración responsable en la que declare cumplir con el Código Ético. La falta de suscripción de la declaración responsable determinará la retirada del reconocimiento de los programas de formación.

Las entidades acreditadas y las entidades de formación deberán, en el plazo de 3 meses desde la publicación del presente Esquema, presentar una declaración responsable en la que declaren cumplir con los requisitos relativos a la independencia e imparcialidad recogidos en el mismo.

ANEXOS

Anexo I. Condiciones para la justificación de los prerrequisitos y del proceso de reconocimiento de los programas de formación

Anexo II. Marca del Esquema

- Anexo II.A. Normas de uso de la Marca del Esquema
- Anexo II.B. Modelo de contrato de uso de la Marca del Esquema

Anexo III. Código Ético EC y EF

Anexo IV. Código Ético DPD

Anexo V. Programa (temario) del Esquema

Anexo VI. Procedimiento de selección y designación de evaluadores

Anexo VII. Modelo de informe de los resultados del examen

Anexo VIII. Modelo de documento justificativo de la certificación

ANEXO I

CONDICIONES PARA LA JUSTIFICACIÓN DE LOS PRERREQUISITOS Y DEL PROCESO DE RECONOCIMIENTO DE LOS PROGRAMAS DE FORMACIÓN

I.- CONDICIONES PARA LA JUSTIFICACIÓN DE LOS PRERREQUISITOS.

Las personas candidatas a concurrir en los procesos de certificación como DPD deberán acreditar los requisitos de formación y experiencia profesional en los siguientes términos:

A. FORMACIÓN.

Aportar certificado de haber recibido la formación necesaria y reconocida en relación con las materias objeto del programa del Esquema para poder presentarse al examen, en el que conste:

- Entidad de formación que emite el certificado.
- Entidad de certificación que ha reconocido el programa.
- La formación recibida (60, 100 o 180 horas).
- La distribución de las horas de formación del programa conforme al porcentaje establecido para cada uno de los dominios del programa del Esquema. Un programa de formación puede estar formado por varios cursos.
    - Para la formación de 60 horas la distribución será la siguiente:
        - Dominio 1 - 30 horas, Dominio 2 – 18 horas, Dominio 3 – 12 horas
    - Para la formación de 100 horas la distribución será la siguiente:
        - Dominio 1 - 50 horas, Dominio 2 – 30 horas, Dominio 3 – 20 horas
    - Para la formación de 180 horas la distribución será la siguiente:
        - Dominio 1 - 90 horas, Dominio 2 – 54 horas, Dominio 3 – 36 horas

Para la formación expresada en créditos ECTS[1] o LRU[2] (referida a formación universitaria, incluso con prácticas o trabajo fin de carrera) se considera que 1 ECTS equivale a 25 horas y 1 LRU a 10 horas.

En el cómputo de horas para la justificación de la formación adquirida respecto de los dominios 2 y 3 será valorable tanto la obtenida antes como después de la publicación del RGPD (BOE de

[1] Créditos según el Sistema Europeo de Transferencia de Créditos.
[2] Créditos según la Ley de Reforma Universitaria de 1983.

4 de mayo de 2016). Por tanto, el candidato no necesita cursar un programa de formación completo de 60, 100 o 180, sino tan sólo aquella materia que necesite para cumplimentar las horas de formación requeridas siguiendo los criterios del Esquema.

B. EXPERIENCIA LABORAL O PROFESIONAL.

Justificar experiencia laboral o profesional de dos, tres, o cinco años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD (obtenida antes o después de la publicación del RGPD). Para ello el candidato deberá aportar:

a) Trabajador por cuenta ajena que ha desempeñado sus funciones dentro de una empresa como asalariado: certificado de la vida laboral y certificado de la empresa donde consten las tareas desempeñadas en relación con la materia de protección de datos, fecha de inicio y fecha de finalización.

b) Trabajador autónomo que presta sus servicios a distintos clientes: certificado de la vida laboral y certificado de los clientes donde consten las tareas desempeñadas en relación con la materia de protección de datos, fecha de inicio y de finalización de los servicios prestados, debiendo sumar en total los años requeridos de experiencia.

c) Trabajador en empresa de consultoría, es decir, el empleado de una consultora que presta servicios a distintas empresas: certificado de la vida laboral y certificado de la consultora donde consten las tareas desempeñadas en relación con la materia de protección de datos, fecha de inicio y de finalización de los trabajos realizados.

d) Trabajador independiente que presta sus servicios a empresas de consultoría: certificado de vida laboral y certificado de la consultora.

Los años de experiencia (2, 3, o 5), son a tiempo completo. La dedicación se calcula tomando como base que la jornada anual de 225 días, y que una jornada se considera completa si justifica 8 horas de dedicación.

Se valorará especialmente la experiencia en el tratamiento de datos personales de alto riesgo con el doble de tiempo que los años de experiencia en el tratamiento de datos personales que no suponga ese nivel de riesgo.

En el caso de que la experiencia no sea de un año completo, se valorará la experiencia que iguale o supere los seis meses con la mitad de la puntuación anual.

Sólo en caso de no alcanzar la experiencia requerida se podrá convalidar hasta un año de experiencia mediante convalidación de méritos adicionales, es decir, hasta 60 puntos.

Como experiencia laboral se considerará también la formación impartida y, en concreto, se valorará con el doble de horas de la formación recibida.

La formación impartida en una materia específica sólo se considerará aceptada una de las ediciones impartidas, en caso de haber más de una con el mismo título y temario.

Para la valoración de la experiencia se aplicará el baremo de la tabla 1.

Tabla 1

Formación	Experiencia	Puntuación de año experiencia	Mínimo puntuación de años de experiencia
-	5 años	60 puntos	300 puntos
60 horas	3 años	60 puntos	180 puntos
100 horas	2 años	60 puntos	120 puntos
180 horas	-		

C. CONVALIDACION DE MÉRITOS ADICIONALES

Si se alcanza la puntuación requerida por los prerrequisitos de experiencia profesional no será necesario valorar ningún mérito adicional. Sólo en el caso en que no se supere la puntuación mínima requerida por falta de años de experiencia se utilizará la siguiente tabla de méritos para complementar la puntuación.

No se evaluarán como méritos aspectos considerados ya como prerrequisitos.

Para la valoración de los méritos adicionales se aplicará el baremo de la tabla 2.

Tabla 2

Categoría	Puntuación Máxima	Mérito	Puntos unitarios[3]	Máx.
Formación universitaria específica o complementaria en protección de datos o privacidad, según EEES.[4]	30	Grado, diplomatura o ingeniería técnica	6	12
		Postgrado o Máster título propio	6	12
		Posgrado oficial	8	16
		Máster oficial	10	20
		Doctorado	9	9
Formación específica o complementaria, en protección de datos o privacidad.	50	Asistencia a cursos, seminarios, eventos, actos o congresos organizados o expresamente reconocidos por Autoridades o Entidades de Certificación de Protección de Datos (mínimo 1 crédito o 10 h.)	1	25
		Asistencia a cursos o seminarios no universitarios organizados por organizaciones profesionales (mínimo 2 créditos o 20 h.)	0,20	10
		Asistencia a cursos o seminarios universitarios (mínimo 2 créditos o 20 h.)	0,50	10

[3] Atribuibles a cada mérito individualmente considerado. En casos específicos como la asistencia a eventos se considerará que se alcanza una unidad cuando se acredite el total de horas mínimo reconocido.
[4] Según EEES: Espacio Europeo de Educación Superior.

Categoría	Puntuación Máxima	Mérito	Puntos unitarios[3]	Máx.
		Asistencia a eventos, actos o congresos propios de la especialidad que deberán sumar al menos 20 h. al año.	0,50	5
Trabajo fin de curso en temas de protección de datos o privacidad.	5	Superación de trabajo fin de curso con una dedicación de al menos 40 horas.	1	5
Prácticas en empresas en temas de protección de datos o privacidad.	5	Realización de prácticas en empresas con una dedicación de al menos 40 horas.	1	5
Actividad docente relacionada con la materia de protección de datos o privacidad.	30	Docencia en titulaciones universitarias (por cada 10 h.)	0,5	10
		Profesor en cursos/seminarios de nivel básico (por cada 20 h.) Profesor cursos y seminarios de especialización (por cada 10 h.)	0,2	5
		Profesor en cursos de Entidades de Certificación (por cada 10 h.)	0,5	10
		Conferenciante, ponente o comunicante en congresos (por evento)	0,1	5
Actividad investigadora y publicaciones en temas de protección de datos o privacidad.	20	Autoría o coautoría de libros	2,5	8
		Autoría o coautoría de capítulos de libro, actas oficiales de congresos y equivalentes.	0,5	5
		Autoría o coautoría de artículos en revistas y publicaciones especializadas.	0,25	5
		Autoría o coautoría de aportaciones en medios de comunicación y blogs.	0,10	2
Premios de protección de datos o privacidad.	10	Premios y reconocimientos profesionales o similar.	5	10

Categoría	Puntuación Máxima	Mérito	Puntos unitarios[3]	Máx.
Certificaciones en materias de protección de datos o privacidad (en vigor).	10	ACP-DPO de APEP, CDPP de ISMS FORUM[5], ECPC-B DPO de Universidad de Maastricht, DPO de EIPA (European Institute of Public Administration) o similar.	5	10
Otras certificaciones en materias relacionadas (en vigor).	10	ACP-B/ACP-CL/ACP-CT/ACP-AL/ACP-AT de APEP, CDPP de ISMS FORUM[6], CISA/CISM/CRISC de ISACA, CISSP de Certified Information Systems Security Professional (ISC)[2], CIPP/CIPT de IAPP (International Association of Privacy Professionals), Auditor ISO 27001 o similar.	2	10

II.- PROCESO DE RECONOCIMIENTO DE LOS PROGRAMAS DE FORMACIÓN.

Las Entidades de Formación deberán solicitar a las Entidades de Certificación el reconocimiento de sus programas de formación siguiendo los requisitos establecidos en este Anexo. Si fuera preciso, se publicarán por la AEPD los requisitos de reconocimiento exigibles, tanto a los programas de formación como a las entidades que la imparten, en lo relativo a contenido, duración mínima de la formación, método de validación, requisitos relativos al personal formador, a los medios o las instalaciones, aprovechamiento, etc.

Las EC reconocerán los programas de formación de las EF conforme a los siguientes requisitos:

- Duración (60, 100 o 180 horas).
- Materia impartida de acuerdo con el programa definido en el Esquema.
- Método de validación mediante la superación de un examen (no basta con justificar la asistencia a la formación).
- Metodología didáctica que incluya impartición de conocimientos teóricos, realización de ejercicios prácticos y desarrollo de ejercicios colaborativos con un resultado y valor expositivo (trabajos en grupo que incluyan exposiciones y debates, ya sean presenciales y/o telepresenciales).

[5] Nuevo CDPP desde diciembre de 2016.
[6] CDPP anterior a diciembre de 2016.

A estos efectos, las personas que impartan la formación deberán disponer de los conocimientos y experiencia profesional equivalente o superior a la exigida al candidato a certificar y con capacidad de valorar la capacitación de los alumnos. No podrán compatibilizar la formación con la elaboración de preguntas ni con la función de evaluador en las entidades de certificación.

La distribución de las horas de los programas de formación deberá ajustarse a los siguientes criterios:

- Para la formación de 60 horas:
    - Dominio 1 - 30 horas.
    - Dominio 2 – 18 horas.
    - Dominio 3 – 12 horas
- Para la formación de 100 horas:
    - Dominio 1 - 50 horas.
    - Dominio 2 – 30 horas.
    - Dominio 3 – 20 horas.
- Para la formación de 180 horas:
    - Dominio 1 - 90 horas.
    - Dominio 2 – 54 horas.
    - Dominio 3 – 36 horas.

Para la formación expresada en créditos ECTS[7] o LRU[8] (referida a formación universitaria, incluso con prácticas o trabajo fin de carrera) se considera que 1 ECTS equivale a 25 horas y 1 LRU a 10 horas.

Los programas de formación reconocidos por las EC tienen validez a partir de la fecha del reconocimiento y serán válidas aquellas formaciones que se inicien a partir de esa fecha. No se considera válidas ediciones anteriores a la fecha del reconocimiento.

Las EF a las que se les haya reconocido su programa de formación por las entidades que se encuentren en proceso de concesión de la acreditación no podrán dar comienzo a la formación hasta que no hayan sido acreditadas por ENAC.

[7] Créditos según el Sistema Europeo de Transferencia de Créditos.
[8] Créditos según la Ley de Reforma Universitaria de 1983.

El reconocimiento de un programa de formación por parte de una EC tendrá validez para las restantes EC al objeto de acreditar la formación como prerrequisito de acceso al examen en cualquier otra EC.

Por tanto, la Entidad de Formación, una vez reconocidos sus programas de formación por una EC, no necesitará el reconocimiento de otras Entidades de Certificación.

Las EC emitirán a la EF un certificado de reconocimiento de formación en el que conste:

- Nombre de la Entidad de Certificación.
- Nombre de la Entidad de Formación con identificación de su página web.
- Nombre del programa reconocido.
- Fecha del reconocimiento.
- Duración (60, 100 o 180 horas) y criterios de superación del mismo.
- Materia impartida y distribución de horas por cada uno de los tres dominios del temario.
- Formato del programa (online o presencial).

El certificado de reconocimiento incluirá la siguiente cláusula:

> «El reconocimiento mantendrá su vigencia mientras no sean modificados los requisitos verificados para su obtención de conformidad con el Esquema AEPD-DPD en su versión vigente (programa, distribución por dominio, metodología docente y método de validación), o el propio esquema en lo que le pudiera afectar.»

El reconocimiento de programas de formación no debe comprometer la independencia e imparcialidad, ni reducir los requisitos de la evaluación y la certificación, razón por la que las EC no pueden ofrecer formación bajo el Esquema, utilizando la misma marca comercial o logo, tampoco marcas o logos que puedan inducir a confusión pues constituye una amenaza a la necesaria imparcialidad.

Las EC publicarán en su página web la siguiente información sobre los programas de formación reconocidos y de los que hubieran perdido su vigencia:

- Nombre de la Entidad de Formación con identificación de su página web (la dirección web debe apuntar directamente a la zona de la página web donde se oferta la formación).
- Nombre del programa reconocido.
- Fecha del reconocimiento.
- Duración (60, 100 o 180 horas) y criterios de superación del mismo.
- Materia impartida y distribución de horas por cada uno de los tres dominios del temario.
- Formato del programa (online o presencial).
- En su caso, fecha y motivos de la pérdida de vigencia del reconocimiento.

Las EF deberán publicar en su página web información clara y transparente sobre los programas de formación reconocidos incluyendo los siguientes datos:

- Nombre completo de la Entidad de Formación
- Nombre de la EC que ha reconocido los programas
- Nombre del programa reconocido
- Fecha de realización del programa
- Duración y criterios de superación del programa
- Materia impartida y distribución de horas por cada uno de los tres dominios del temario
- Formato del programa (online o presencial)
- Relación de los profesores que imparten cada uno de los epígrafes por dominio
- Currículum actualizado de los profesores

Las EF emitirán a los alumnos de sus programas de formación, un certificado en el que conste:

- Nombre de la Entidad de Formación
- Nombre del programa reconocido
- Fecha de realización del programa
- Duración y criterios de superación del programa
- Materia impartida y distribución de horas por cada uno de los tres dominios del temario.
- Formato del programa (online o presencial)

La AEPD publicará en su página web los programas de formación reconocidos, para ello las EC remitirán dicha información por el método que aquélla designe. Las EC son responsables de mantener la relación de dichos programas actualizada.

Las EC vigilarán que los procesos de formación se desarrollen de acuerdo con la actividad de formación reconocida, que los mismos sean publicitados con transparencia y que, en ningún caso, se produzca un uso inadecuado de la Marca y los logos de las entidades que participan en el Esquema. Con carácter periódico, y al menos anualmente, deberán llevar a cabo actividades de control de los programas formativos reconocidos dirigidas a conseguir una auténtica cualificación de los candidatos y evitar que se focalicen en un simple entrenamiento para superar el examen más que en su formación. Asimismo, deberán informar a las EF de que tanto ENAC como personal técnico de la AEPD pueden asistir de manera no anunciada a los cursos que impartan a fin de evaluar la eficacia de los sistemas de control establecidos por las EC.

Para que las EF puedan mejorar y valorar la formación impartida, las EC que han reconocido sus programas pueden remitirles información estadística sobre el número de aprobados en cada convocatoria, con distribución de los resultados por dominios o epígrafes. Esta información es confidencial, las EC sólo pueden facilitarla a las EF cuyos programas hayan reconocido y deben velar porque las EF no se intercambien este tipo de información. Las EF no pueden publicar esta información en su página web ni utilizarla a efectos comerciales.

La AEPD se reserva el derecho de solicitar en cualquier momento a las EF la entrega de sus programas de formación para su verificación y, en caso de no estar conformes con el Esquema, podrán revocarlos de forma motivada. Asimismo, podrán realizar las pruebas pertinentes para comprobar la rigurosidad de la formación impartida y de las pruebas realizadas a sus alumnos para superar la formación.

En garantía de la independencia e imparcialidad, las EC no pueden comercializar el temario formativo incluido en el Anexo IV del Esquema con las EF, ni los profesores que imparten alguna materia en programas formativos reconocidos bajo el Esquema AEPD-DPD pueden ser evaluadores del Esquema de certificación.

El incumplimiento de los requisitos establecidos para el reconocimiento de los programas de formación de las EF y su control por parte de las EC pueden ser motivo de resolución del contrato de uso de marca (cláusula 5.4 y Anexo II).

Las Universidades Españolas, públicas o privadas, podrán solicitar a la AEPD el reconocimiento de sus programas de postgrado (Máster), tanto los que estén certificados por la Agencia Nacional de Evaluación de la Calidad y Acreditación (ANECA) como los Másteres propios. El reconocimiento se realizará siempre que el Máster cumpla con los requisitos establecidos en el Esquema.

En la solicitud de reconocimiento, la Universidad deberá indicar qué programa del Esquema desea que sea reconocido (180, 100 o 60 horas) y, en función del mismo, ajustar el temario del Máster a los dominios según la distribución detallada atendiendo a los dominios definidos en el Esquema. La Universidad debe adjuntar, junto a su solicitud, un informe justificativo en el que se indique con detalle la correspondencia de los contenidos del Máster con relación al programa del Esquema que desea reconocer.

ANEXO II.A

NORMAS DE USO DE LA MARCA DEL ESQUEMA

1. LA MARCA DEL ESQUEMA.

Al objeto de que el mercado sea capaz de identificar la certificación de personas como "Delegado de Protección de Datos" (DPD) que impulsa la AEPD, se crea la Marca del Esquema AEPD-DPD.

La Marca del Esquema es el símbolo usado por los Entidades de Certificación, las Entidades de Formación y las personas certificadas como Delegados de Protección de Datos para hacer público este hecho e identificarlos como agentes del Esquema.

No podrá ser usada por entidades o personas distintas de las descritas en el párrafo anterior, ni tampoco por ninguna entidad interesada en acreditarse como entidad de certificación mientras esté en proceso de evaluación.

El diseño de la Marca del Esquema se muestra al final de este Anexo.

2. REGLAS DE USO.

La AEPD concederá licencia para el uso de la Marca, mediante contrato con las Entidades de Certificación, sujeta a las siguientes reglas:

a) Se usará siempre claramente asociada al nombre o logotipo del agente autorizado.

b) Las EC y EF podrán emplearla exclusivamente en documentos o soportes de tipo publicitario del servicio que presten en el marco del Esquema (folletos, páginas web, etc.), de forma que quede clara su vinculación únicamente con el servicio prestado dentro del Esquema y no con cualquier otro servicio similar que se oferte al mercado.

c) Los DPD certificados podrán usarla exclusivamente en documentos o soportes de tipo publicitario del servicio que presten como DPD (tarjetas de visita, folletos, páginas web, etc.) y no de cualquier otro servicio similar cuya prestación puedan ofrecer al mercado.

d) Las Entidades de certificación dejarán de emplear la Marca del Esquema cuando finalice o resuelva el contrato de licencia de uso, así como en caso de suspensión o retirada de la acreditación a las EC por parte de ENAC. En estos casos las personas certificadas por dichas entidades podrán seguir haciendo uso de la Marca, hasta la renovación de la certificación, en cuyo caso, pasarán a utilizar la de la EC que se la renueve.

e) Las Entidades de Formación dejarán de utilizar el uso de la Marca cuando haya finalizado la validez del reconocimiento de sus programas de formación, o se haya revocado. En el

caso de que las EC deban dejar de usar la marca, las EF podrán seguir usándola en aquellos programas de formación que estén en curso en ese momento, en otro caso deberán obtener el reconocimiento de sus programas de otra EC para hacer uso de la Marca.

Las EC son responsables de que tanto ellas como las EF cuyos programas de formación han reconocido, y los DPD a los que hayan certificado usan la Marca siguiendo estas normas. En caso de detectar un mal uso de la Marca deberán adoptar las medidas oportunas, incluidas la revocación del reconocimiento de los programas de formación y la suspensión o retirada de la certificación.

La infracción de las obligaciones de las EC respecto a la vigilancia y control del uso de la Marca por las EF y los DPD podrá dar lugar a la resolución del contrato de uso de la Marca.

EN EL RECUADRO CENTRAL SE INCLUIRÁ:

- PARA LAS ENTIDADES DE CERTIFICACIÓN, LA FECHA EN QUE SE OBTUVO LA ACREDITACIÓN
- PARA LAS ENTIDADES DE FORMACIÓN, LA FECHA EN QUE SE OBTUVO EL RECONOCIMIENTO DE LA FORMACIÓN
- PARA LOS DELEGADOS DE PROTECCIÓN DE DATOS, LA FECHA EN QUE OBTUVO LA CERTIFICACIÓN

ANEXO II.B

MODELO DE CONTRATO DE USO DE LA MARCA DEL ESQUEMA ENTRE LA AEPD Y LOS AGENTES DEL ESQUEMA

En Madrid, a de de 20..

REUNIDOS

De una parte,

De otra parte,

Reconociéndose mutuamente la capacidad legal necesaria para el otorgamiento del presente contrato,

EXPONEN

I. Que, al objeto de que el mercado sea capaz de identificar la certificación de personas como “Delegado de Protección de Datos” (DPD) que impulsa la AEPD, se ha creado la Marca del Esquema AEPD-DPD.

II. Que la Marca del Esquema es el símbolo usado por los Agentes del Esquema y las personas certificadas para hacer público este hecho.

III. Que la marca del Esquema es propiedad de la AEPD y solo puede ser usada bajo la responsabilidad de la Entidad de certificación abajo firmante en las condiciones establecidas en las Normas de uso publicadas por la AEPD como parte del Esquema de certificación de delegados de la Agencia Española de Protección de Datos (Esquema AEPD-DPD).

IV. Que la Entidad de certificación abajo firmante está interesada en operar en el Esquema AEPD-DPD.

V. Que la firma del contrato de uso de la marca es una condición para operar dentro del Esquema, debiendo firmarse el mismo con carácter previo a la solicitud de la acreditación a ENAC, a quién deberá aportarse copia de este contrato.

VI. Que ambas partes han acordado proceder a la firma del presente Contrato de uso de la marca con sujeción a las siguientes:

CLÁUSULAS

PRIMERA. Objeto

La AEPD cede a la Entidad de certificación los derechos de uso de la marca del Esquema en las condiciones establecidas en las Normas de uso de la marca recogidas en el Anexo II.A y en la cláusula 5.4 del Esquema AEPD-DPD.

SEGUNDA. Condición suspensiva.

El uso de la marca del Esquema queda condicionado al otorgamiento de la acreditación por ENAC conforme al Procedimiento de Acreditación.

La Entidad de Certificación deberá comunicar a la AEPD la obtención de la acreditación al objeto de que la AEPD le suministre formalmente el correspondiente archivo de la marca, momento a partir del cual podrá comenzar el uso de la misma.

TERCERA. Responsabilidad de la Entidad de Certificación.

La Entidad de certificación es responsable de:

a) Ejercer un adecuado control del uso de la marca conforme a las condiciones establecidas en las Normas de uso de la marca recogidas en el Anexo II.A y en la cláusula 5.4 del esquema AEPD-DPD, tanto por sí misma como por las Entidades de Formación que reconozca y los DPD que certifique, asumiendo las consecuencias establecidas en el Esquema en caso de incumplimiento de dicha obligación.

b) Informar a las Entidades de Formación reconocidas de las reglas de uso que le son de aplicación y de su obligación de cesar de usar la marca del esquema en caso de resolución de este contrato y que dicha obligación esté establecida de manera contractual con las EF. Adicionalmente la EC se compromete a tomar medidas legales contra las EF en caso de que éstas incumplan dicha obligación.

c) Informar a los DPD certificados sobre las Normas de uso que les son de aplicación, así como de las consecuencias de un uso incorrecto

CUARTA. RESOLUCIÓN DEL CONTRATO.

1. Son causas de resolución del presente contrato:

a) El mutuo acuerdo de las partes.
b) El transcurso del plazo de seis meses desde la solicitud de acreditación a ENAC sin que se haya obtenido la misma, por causas imputables a la Entidad de certificación.
c) La retirada de la acreditación.

2. Asimismo, podrá dar lugar a la resolución del contrato, motivadamente y previa audiencia de la Entidad de certificación:

a) La suspensión de la acreditación.

b) El incumplimiento del código ético.

c) El incumplimiento por la Entidad de Certificación de su deber de control del uso de la Marca respecto de las Entidades de Formación que ha reconocido y los DPD que ha certificado.

d) Cualquier otro incumplimiento de las obligaciones establecidas en el presente contrato.

e) Cualquier otra causa distinta de las anteriores prevista en la legislación vigente que fuera de aplicación.

3. La resolución del contrato implica que la entidad no pueda ofrecer los servicios de certificación dentro del Esquema, dando lugar a la extinción de la condición de Agente del Esquema y a la indemnización de los daños y perjuicios causados.

4. Resuelto el contrato, la AEPD no firmará un nuevo contrato de uso de la marca con dicha entidad hasta transcurridos dos años, a contar desde la resolución.

QUINTA. Jurisdicción competente.

Las controversias que pudieran surgir entre las partes como consecuencia de la interpretación o ejecución de este contrato serán de conocimiento y competencia del orden jurisdiccional contencioso-administrativo.

ANEXO III

CÓDIGO ÉTICO PARA LAS ENTIDADES QUE SOLICITEN LA ACREDITACIÓN COMO ENTIDADES CERTIFICADORAS DE DELEGADOS DE PROTECCIÓN DE DATOS CONFORME AL ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN Y LAS ENTIDADES QUE OFREZCAN FORMACIÓN

PREÁMBULO

El presente Código constituye una declaración expresa de los valores y principios que, basados en la normativa aplicable y en los requisitos del Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (AEPD-DPD), deben presidir y guiar el comportamiento de aquellas entidades y empresas (en adelante, entidades interesadas) que soliciten de la Empresa Nacional de Acreditación (ENAC) la acreditación para ser entidades certificadoras (en adelante, EC) de Delegados de Protección de Datos, conforme al Esquema AEPD-DPD, en el ejercicio y desempeño de su actividad profesional.

El código ético recoge un conjunto de principios y valores (legalidad, integridad, honorabilidad, competencia leal, profesionalidad, responsabilidad, imparcialidad, transparencia y confidencialidad) que provienen de las obligaciones que establecen las distintas normativas que son de aplicación a la actividad de las entidades que solicitan la acreditación de EC a ENAC, así como de las recogidas en el Esquema AEPD-DPD.

Su observancia se fundamenta en la diligencia debida para su cumplimiento con la finalidad de proporcionar confianza y garantía de un comportamiento absolutamente responsable con la legalidad vigente en sus relaciones con empleados, proveedores, clientes y cualesquiera terceros con los que se relacionen, tanto de ámbito público como privado, incluyendo la sociedad en general.

El objetivo del presente código es procurar un comportamiento profesional por parte de las entidades interesadas: de sus directivos, empleados, apoderados, representantes y colaboradores, que se aleje de conductas y hechos contrarios a los principios y valores que recoge.

El código ético, que las entidades interesadas vienen obligadas a suscribir con carácter previo a la presentación de la solicitud de acreditación, implica el compromiso de actuar conforme a sus principios y valores durante el procedimiento de acreditación como EC por ENAC y durante el ejercicio de su actividad como EC una vez que como tal hayan sido reconocidas.

Para que el código sea efectivo y proporcione confianza y seguridad a los que se relacionen o hayan de relacionarse con las entidades interesadas de un comportamiento ético, éstas han de

proceder a su difusión entre directivos, empleados, apoderados, representantes y colaboradores; establecer procedimientos y estructuras para la comunicación y gestión de reclamaciones; y para la supervisión y control de su observancia, funciones que, en su caso, también podrán ser realizadas por la AEPD en garantía del buen funcionamiento del Esquema AEPD-DPD.

El código ético se aplica igualmente a las entidades de formación, cuyo comportamiento en el marco del Esquema AEPD-DPD ha de observar los principios y valores que contiene.

ARTÍCULO I. AMBITO DE APLICACIÓN

Los principios y valores contenidos en el presente código ético son de obligada observancia y cumplimiento para las entidades que soliciten de la Empresa Nacional de Acreditación (ENAC) ser acreditadas para certificar DPD con arreglo al Esquema AEPD-DPD, así como por sus directivos, empleados, apoderados, representantes y colaboradores, desde el mismo momento de presentación de la solicitud y durante el ejercicio de su actividad como EC en el marco del Esquema AEPD-DPD.

Será de aplicación para todas las sociedades que formen parte de las entidades interesadas, incluyendo sus directivos, empleados, apoderados, representantes y colaboradores.

El código ético será de aplicación a las entidades de formación, a sus directivos, empleados, apoderados, representantes y colaboradores.

ARTÍCULO II. PRINCIPIOS DE ACTUACIÓN

Las entidades interesadas y sus sociedades, sus directivos, empleados, apoderados, representantes y apoderados en el ejercicio de sus actividades se comportarán con sujeción a los siguientes principios:

- **Legalidad**, las entidades interesadas cumplirán estrictamente con la legislación y la normativa vigente en cada momento, y especialmente con lo establecido en el Esquema AEPD-DPD, al objeto de evitar que se lleve a cabo cualquier actividad ilícita y, en particular, las prácticas o declaraciones que de cualquier manera supongan un perjuicio para la ENAC, AEPD, el Esquema AEPD-DPD, o a cualquiera de sus actores.

  Las entidades interesadas se comprometen a adoptar las medidas necesarias para que sus directivos, empleados, apoderados, representantes y colaboradores conozcan la normativa aplicable, incluidos los principios y valores del código ético y los puedan observar.

- **Integridad,** las entidades interesadas desarrollarán sus actividades de en todo momento con ética profesional, de manera honrada, profesional y de buena fe, evitando los conflictos de intereses.

- **Honorabilidad,** las entidades interesadas no deberán haber sido objeto de sanción en cualquiera de los ámbitos de su actividad y ejercicio profesional durante los tres (3) años anteriores a la presentación de la solicitud de acreditación, ni ser sancionadas durante su desempeño como EC**.**

- **Competencia leal**, las entidades interesadas desarrollarán su actividad profesional de manera leal, sin permitir comportamientos engañosos, fraudulentos, o maliciosos.

  En protección de datos evitarán las prácticas agresivas como:

  Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

  Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

  Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

  Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

  Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

- **Responsabilidad**, en el desarrollo de sus actividades profesionales, las entidades interesadas asumirán las actividades de colaboración que le requiera la AEPD y demás autoridades públicas, así como el resto de las entidades del Esquema AEPD-DPD para su correcto desarrollo y mantenimiento, evitando cualquier conducta que perjudique su reputación.

- **Imparcialidad**, las entidades interesadas actuarán con objetividad en sus relaciones con terceros, sin aceptar presiones o influencias de terceros que pudieran cuestionar su integridad profesional, o la de sus directivos, empleados, apoderados, representantes y colaboradores, en particular con las entidades de formación del Esquema AEPD -DPD.

- **Transparencia**, las entidades interesadas actuarán con transparencia en el ejercicio de su actividad profesional, en concreto en el ámbito del Esquema AEPD-DPD que exige:

    - Informar a todas las partes interesadas de forma clara, precisa y suficiente de todos los aspectos que confluyen en el ejercicio profesional como EC, siempre y cuando los mismos no estén sujetos al régimen de confidencialidad, en cuyo caso tendrán carácter reservado y no podrán ser divulgados.

    - Facilitar a todas las partes interesadas con claridad, precisión y suficiencia toda la información relevante sobre el proceso de certificación y sobre el estado de la acreditación

- **Confidencialidad**, las entidades interesadas respetarán y guardarán la necesaria protección y reserva de la información a la que pudiera tener acceso por razón de su actividad como EC, salvaguardando los derechos legítimos de todas las partes interesadas. Dicha información no será utilizada para su beneficio ni de su personal, ni revelada a partes inapropiadas.

ARTÍCULO III. RELACIONES CON EL PERSONAL DE LA ORGANIZACIÓN

En sus relaciones con sus empleados, directivos y colaboradores, las entidades interesadas:

- Pondrán los medios necesarios para comunicar y difundir el código ético entre todos sus empleados.

- Evitarán las situaciones que puedan dar lugar a conflictos de intereses con las actividades de la organización.

- Establecerán procedimientos que permitan la notificación de conductas contrarias al código ético y al esquema AEPD-DPD.

- Vigilarán que el personal a su cargo no lleve a cabo actividades ilícitas ni conductas contrarias al código ético y al Esquema AEPD-DPD.

- Asumirán la responsabilidad de la actuación de sus directivos, empleados apoderados, representantes y colaboradores.

ARTÍCULO IV. RELACIONES CON COLABORADORES EXTERNOS, PROVEEDORES Y CLIENTES

Las entidades interesadas:

- Establecerán unas relaciones basadas en el respeto a la legalidad vigente, el Esquema AEPD-DPD, el comportamiento ético, la lealtad, la buena fe, la confianza, respeto y transparencia.
- Actuarán con imparcialidad y objetividad en los procesos de selección de colaboradores, aplicando criterios debidamente documentados de competencia y calidad, evitando en todo momento la colisión de intereses, en particular con las entidades de formación.
- Garantizarán documentalmente una absoluta independencia con las entidades que presten formación a los candidatos a obtener la certificación.
- Darán a conocer el contenido del presente código deontológico.

ARTÍCULO V. RELACIONES CON CLIENTES

En sus relaciones con los clientes, las entidades interesadas:

- Darán a conocer el contenido del presente código deontológico.
- Actuarán de forma ética, íntegra, de buena fe y profesional, teniendo como objetivo la consecución de un alto nivel de calidad en la prestación de sus servicios, buscando el desarrollo de unas relaciones basadas en la confianza, seguridad y en el respeto mutuo.
- Salvaguardarán siempre la independencia, evitando que su actuación profesional se vea influida por vinculaciones económicas, familiares y de amistad con los clientes, o de sus relaciones profesionales al margen de la actividad de las EC, no debiendo aceptar regalos o favores de cualquier naturaleza de parte de éstos o de sus representantes.
- No efectuarán ni aceptarán, directa ni indirectamente, ningún pago o servicio de más valor ni distinto al establecido para el servicio proporcionado.

- Pondrán en conocimiento del cliente cualquier situación que pueda dar lugar a un conflicto de intereses en la prestación de sus servicios antes de asumir un encargo profesional.

- No realizarán ninguna actividad promocional (publicidad, material informativo, u otra) que pueda inducir a los clientes a una incorrecta interpretación del significado de la Acreditación bajo el Esquema AEPD-DPD, o a unas expectativas que no respondan a la situación real.

- No ofrecerán la formación requerida en el Esquema AEPD-DPD ni publicitarán, en su página web, o en otros medios, cursos relacionados con el Esquema AEPD-DPD.

- No realizarán ofertas, descuentos u otros beneficios a los candidatos a obtener la certificación como DPD por provenir de programas de formación determinados.

ARTÍCULO VI. RELACIÓN CON LAS AUTORIDADES Y ORGANISMOS PÚBLICOS

Las relaciones con las instituciones, organismos y Administraciones públicas (estatal, autonómicas y locales), especialmente con la AEPD, se desarrollarán bajo el principio de máxima colaboración y escrupuloso cumplimiento de sus resoluciones. Las comunicaciones, requerimientos y solicitudes de información que las entidades interesadas reciban de autoridades y organismos públicos deberán ser atendidas con diligencia, en los plazos establecidos para ello.

ARTÍCULO VII. CONTROL DE APLICACIÓN DEL CÓDIGO

Las Entidades de Certificación y de Formación permitirán el acceso al registro de las reclamaciones relacionadas con el código ético a ENAC y a la AEPD y colaborarán plenamente con cualquier actuación o investigación sobre su cumplimiento se lleve a cabo por ENAC o la AEPD.

ARTÍCULO VIII. ACEPTACIÓN E INTERPRETACIÓN DEL CÓDIGO ÉTICO

El Esquema AEPD-DPD exige a las entidades interesadas un alto nivel de compromiso en el cumplimiento del código ético.

Las entidades interesadas se comprometen a la suscripción y aplicación del presente código ético que forma parte del Esquema AEPD-DPD.

Cualquier duda que pueda surgir sobre la interpretación o aplicación del código ético deberá consultarse con la AEPD, quien tiene la obligación de fomentar el conocimiento y cumplimiento del código e interpretarlo en caso de duda.

ARTÍCULO IX. INCUMPLIMIENTO DEL CÓDIGO ÉTICO

La falta de adhesión al código ético, o el incumplimiento de alguno de los compromisos que implica supondrán la resolución del contrato de uso de la Marca.

ARTÍCULO X. RÉGIMEN TRANSITORIO

Las entidades interesadas y aquellas que ya estén acreditación como Entidades de Certificación por ENAC, y las Entidades de Formación deberán suscribir el código ético en los plazos que se establecen en la Disposición Transitoria del Esquema (apartado 10 del Esquema).

ANEXO IV

CÓDIGO ÉTICO DE LAS PERSONAS CERTIFICADAS COMO DELEGADOS DE PROTECCIÓN DE DATOS CONFORME AL ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

PREÁMBULO

El presente Código constituye una declaración expresa de los valores, principios y normas que deben guiar la conducta de las personas certificadas como Delegados de Protección de Datos (DPD), conforme al Esquema de Certificación de la Agencia Española de Protección de Datos (AEPD), en el ejercicio de sus funciones o tareas, y en sus relaciones con otros empleados, como con clientes, proveedores, instituciones públicas y privadas, colaboradores externos y la sociedad en general.

El Código Ético recoge, por tanto, un conjunto de compromisos de integridad, imparcialidad, legalidad, confidencialidad y transparencia que habrán de suscribir ineludiblemente, así como conocer y difundir, quienes pretendan desarrollar su actividad profesional como Delegados de Protección de Datos certificados con arreglo al Esquema de la AEPD.

De este modo, a través del presente Código, se persigue prevenir la comisión de comportamientos contrarios a los criterios que contiene, al tiempo que se diseñan mecanismos de seguimiento y control que garanticen su íntegro cumplimiento por parte de todas aquellas personas que desempeñen su labor profesional como DPD certificados por el Esquema de la AEPD.

Los criterios de conducta recogidos en este Código no pretenden contemplar la totalidad de situaciones o circunstancias con las que los mencionados profesionales se pueden encontrar, sino establecer unas pautas generales de conducta que les orienten en su forma de actuar durante el desempeño de su actividad profesional.

ARTÍCULO I. AMBITO DE APLICACIÓN

Los principios, valores y criterios contenidos en el presente Código Ético son de obligado cumplimiento para los Delegados de Protección de Datos certificados por los organismos de certificación acreditados por la Empresa Nacional de Acreditación (ENAC) con arreglo al Esquema de la AEPD.

ARTÍCULO II. PRINCIPIOS GENERALES

Los DPD certificados en su actividad profesional conforme al esquema de la AEPD llevarán a cabo todas sus actuaciones con sujeción a los siguientes principios:

- **Legalidad e integridad**, cumpliendo estrictamente con la legalidad vigente, en particular la referida a la prestación del servicio, al objeto de evitar que se lleve a cabo cualquier actividad ilícita.

- **Profesionalidad,** desarrollando sus funciones con la debida diligencia y rigor profesional, y manteniendo permanentemente actualizada su capacidad profesional y su formación personal; debiendo comportarse ante las personas, empresas, entidades y clientes de modo escrupulosamente leal e independiente de las limitaciones de cualquiera naturaleza que puedan influir su propia labor y la del personal del que, eventualmente, sea responsable.

- **Responsabilidad** en el desarrollo de su actividad profesional y personal, asumiendo sólo aquellas actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias.

- **Imparcialidad**, actuando con objetividad sin aceptar la influencia de conflictos de intereses u otras circunstancias que pudieran cuestionar la integridad profesional y la de la propia organización a la que pertenece.

- **Transparencia**, informando a todas las partes interesadas de forma clara, precisa y suficiente de todos los aspectos que confluyen en el ejercicio profesional, siempre y cuando los mismos no estén sujetos al régimen de confidencialidad, en cuyo caso tendrán carácter reservado y no podrán ser divulgados.

- **Confidencialidad,** respetando y guardando la necesaria protección y reserva de la información a la que pudiera tener acceso por razón de actividad profesional, salvaguardando los derechos de todas las partes interesadas a su intimidad. Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.

ARTÍCULO III. RELACIONES CON EL PERSONAL DE LA ORGANIZACIÓN

En sus relaciones con el resto de los empleados, directivos y colaboradores de la organización, el Delegado de Protección de Datos:

- Deberá tratar de forma justa y respetuosa al resto de empleados o directivos de su organización.

- Asumirá la responsabilidad de su actuación y la de sus colaboradores, promoviendo su desarrollo profesional a través de la motivación, la formación y la comunicación. En todo caso, la relación con los colaboradores deberá estar presidida por el respeto mutuo y la calidad en la dirección.

- Deberá rechazar cualquier manifestación de acoso físico, psicológico, moral o de abuso de autoridad, así como cualquier otra conducta contraria a generar un entorno de trabajo agradable, saludable y seguro.

- Vigilará que el personal a su cargo no lleve a cabo actividades ilícitas ni conductas contrarias al presente Código Ético.

- Proporcionará siempre toda la información necesaria para el adecuado seguimiento de la actividad, sin ocultar errores o incumplimientos, y procurando subsanar las carencias que se detecten.

ARTÍCULO IV. RELACIONES CON COLABORADORES EXTERNOS Y PROVEEDORES

En sus relaciones con los colaboradores externos y proveedores, el Delegado de Protección de Datos:

- Establecerá unas relaciones basadas en la confianza, respeto, transparencia y el beneficio mutuo.

- Actuará con imparcialidad y objetividad en los procesos de selección de este personal, aplicando criterios de competencia, calidad y coste, evitando en todo momento la colisión de intereses. La contratación de servicios o compra de bienes se deberá realizar con total independencia de decisión y al margen de cualquier vinculación personal, familiar o económica, que pueda poner en duda los criterios seguidos en la selección.

ARTÍCULO V. RELACIONES CON CLIENTES

En sus relaciones con los clientes, el Delegado de Protección de Datos:

- Dará a conocer el contenido del presente código deontológico.
- Actuará de una forma íntegra y profesional, teniendo como objetivo la consecución de un alto nivel de calidad en la prestación de sus servicios, buscando el desarrollo a largo plazo de unas relaciones basadas en la confianza y en el respeto mutuo.
- Salvaguardarán siempre la independencia, evitando que su actuación profesional se vea influenciada por vinculaciones económicas, familiares y de amistad con los clientes, o de sus relaciones profesionales fuera del ámbito de actividad como DPD, no debiendo aceptar honorarios, regalos o favores de cualquier naturaleza de parte de éstos o de sus representantes.
- No efectuará ni aceptará, directa ni indirectamente, ningún pago o servicio de más valor distinto al libremente pactado con su empleador.
- Pondrá en conocimiento del cliente cualquier conflicto de intereses que pueda existir en su prestación profesional relativa a la certificación, antes de asumir un encargo profesional.
- No realizará ninguna actividad promocional (publicidad, material informativo, u otro) que pueda inducir a los clientes a una incorrecta interpretación del significado de las certificaciones bajo el Esquema de la AEPD, o a unas expectativas que no respondan a la situación real.
- Proporcionará a los clientes un formulario para formalizar cualquier queja relacionada con los servicios prestados, que se remitirá tanto a la persona certificada u organización afectada por la queja, como a la Entidad de Certificación.

ARTÍCULO VI. COLABORACIÓN CON LAS ENTIDADES DE CERTIFICACIÓN

Los DPD colaborarán plenamente con cualquier investigación formal sobre infracciones de este código iniciada por las Entidades de Certificación o para resolver casos específicos de reclamación y/o quejas.

A tales efectos, deberán mantener un registro de todas las reclamaciones presentadas contra ellos, por la actividad desarrollada en el ámbito de validez de la certificación y permitir a la Entidad de Certificación el acceso a estos registros. En el plazo de diez días desde la recepción de la reclamación, deberán enviar una comunicación escrita y copia de la reclamación a la Entidad de Certificación.

ARTÍCULO VII. RELACIÓN CON LAS AUTORIDADES Y ADMINISTRACIONES PÚBLICAS

Las relaciones con las instituciones, organismos y administraciones públicas, estatales, autonómicas y locales, especialmente con la Autoridad de Control, se desarrollarán bajo criterios de máxima colaboración y escrupuloso cumplimiento de sus resoluciones. Las comunicaciones, requerimientos y solicitudes de información deberán ser atendidos con diligencia, en los plazos establecidos para ello.

ARTÍCULO VIII. DESEMPEÑO DE OTRAS ACTIVIDADES PROFESIONALES

Los DPD no realizarán actividades competitivas directas o indirectas contra la AEPD y/o la Entidad de Certificación.

A tales efectos, comunicarán a su organización el ejercicio de cualquier otra actividad laboral, profesional o empresarial, remunerada o no, que tenga lugar dentro o fuera del horario de trabajo, o su participación significativa como socio en sociedades o negocios privados, a efectos de evaluar si resultan compatibles con el desarrollo de su actividad o con los fines u objetivos propios de la organización.

ARTÍCULO IX. ACEPTACIÓN E INTERPRETACIÓN DEL CÓDIGO ÉTICO

Los sujetos incluidos en el ámbito de aplicación de este Código tienen el deber de conocerlo y cumplirlo, por lo que deben conocer su contenido y haberlo rubricado. El Esquema de la AEPD exige a los DPD un alto nivel de compromiso en el cumplimiento de este Código Ético.

Cualquier duda que pueda surgir sobre la interpretación o aplicación del presente documento deberá consultarse con la Entidad de Certificación, quien tiene la obligación de fomentar el conocimiento y cumplimiento del Código e interpretarlo en caso de duda.

ARTÍCULO X. INCUMPLIMIENTO DEL CÓDIGO ÉTICO

El incumplimiento de alguno de los principios, valores y criterios contenidos en este Código puede acarrear una investigación de la conducta del titular de la certificación y, en última instancia, medidas disciplinarias por parte del correspondiente organismo de certificación que pueden suponer la suspensión o retirada de la certificación.

ANEXO V

PROGRAMA/TEMARIO DEL ESQUEMA

CONTENIDO

1. Dominio 1. NORMATIVA GENERAL DE PROTECCIÓN DE DATOS.

(Porcentaje temario: 50%)

1.1. Contexto normativo.
1.1.1. Privacidad y protección de datos en el panorama internacional.
1.1.2. La protección de datos en Europa.
1.1.3. La protección de datos en España.
1.1.4. Estándares y buenas prácticas.

1.2. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Fundamentos.
1.2.1. Ámbito de aplicación.
1.2.2. Definiciones.
1.2.3. Sujetos obligados.

1.3. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. LOPD. Principios
1.3.1. El binomio derecho/deber en la protección de datos.
1.3.2. Licitud del tratamiento
1.3.3. Lealtad y transparencia
1.3.4. Limitación de la finalidad
1.3.5. Minimización de datos
1.3.6. Exactitud

1.4. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Legitimación
1.4.1. El consentimiento: otorgamiento y revocación.
1.4.2. El consentimiento informado: finalidad, transparencia, conservación, información y deber de comunicación al interesado.
1.4.3. Consentimiento de los niños.
1.4.4. Categorías especiales de datos.
1.4.5. Datos relativos a infracciones y condenas penales.
1.4.6. Tratamiento que no requiere identificación.
1.4.7. Bases jurídicas distintas del consentimiento.

1.5. Derechos de los individuos.
1.5.1. Transparencia e información
1.5.2. Acceso, rectificación, supresión (olvido).
1.5.3. Oposición
1.5.4. Decisiones individuales automatizadas.

1.5.5. Portabilidad.
1.5.6. Limitación del tratamiento.
1.5.7. Excepciones a los derechos.

1.6. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Medidas de cumplimiento.

1.6.1. Las políticas de protección de datos.
1.6.2. Posición jurídica de los intervinientes. Responsables, co-responsables, encargados, subencargado del tratamiento y sus representantes. Relaciones entre ellos y formalización.
1.6.3. El registro de actividades de tratamiento: identificación y clasificación del tratamiento de datos.

1.7. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Responsabilidad proactiva.

1.7.1. Privacidad desde el diseño y por defecto. Principios fundamentales.
1.7.2. Evaluación de impacto relativa a la protección de datos y consulta previa. Los tratamientos de alto riesgo.
1.7.3. Seguridad de los datos personales. Seguridad técnica y organizativa.
1.7.4. Las violaciones de la seguridad. Notificación de violaciones de seguridad.
1.7.5. El Delegado de Protección de Datos (DPD). Marco normativo.
1.7.6. Códigos de conducta y certificaciones.

1.8. El Reglamento Europeo de Protección de datos. Delegados de Protección de Datos (DPD, DPO, o Data Privacy Officer).

1.8.1. Designación. Proceso de toma de decisión. Formalidades en el nombramiento, renovación y cese. Análisis de conflicto de intereses.
1.8.2. Obligaciones y responsabilidades. Independencia. Identificación y reporte a dirección.
1.8.3. Procedimientos. Colaboración, autorizaciones previas, relación con los interesados y gestión de reclamaciones.
1.8.4. Comunicación con la autoridad de protección de datos.
1.8.5. Competencia profesional. Negociación. Comunicación. Presupuestos.
1.8.6. Formación.
1.8.7. Habilidades personales, trabajo en equipo, liderazgo, gestión de equipos.

1.9. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Transferencias internacionales de datos

1.9.1. El sistema de decisiones de adecuación.
1.9.2. Transferencias mediante garantías adecuadas.
1.9.3. Normas Corporativas Vinculantes
1.9.4. Excepciones.
1.9.5. Autorización de la autoridad de control.
1.9.6. Suspensión temporal
1.9.7. Cláusulas contractuales

1.10. El Reglamento Europeo de Protección de datos y la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales. Autoridades de Control.

1.10.1. Autoridades de Control.
1.10.2. Potestades.
1.10.3. Régimen sancionador.
1.10.4. Comité Europeo de Protección de Datos.
1.10.5. Procedimientos seguidos por la AEPD.
1.10.6. La tutela jurisdiccional.
1.10.7. El derecho de indemnización.

1.11. Directrices de interpretación del RGPD.

1.11.1. Guías del GT art. 29.
1.11.2. Opiniones del Comité Europeo de Protección de Datos
1.11.3. Criterios de órganos jurisdiccionales.

1.12. Normativas sectoriales afectadas por la protección de datos.

1.12.1. Sanitaria, Farmacéutica, Investigación.
1.12.2. Protección de los menores
1.12.3. Solvencia Patrimonial
1.12.4. Telecomunicaciones
1.12.5. Videovigilancia
1.12.6. Seguros
1.12.7. Publicidad, etc.

1.13. Normativa española con implicaciones en protección de datos.

1.13.1. LSSI, Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
1.13.2. LGT, Ley 9/2014, de 9 de mayo, General de Telecomunicaciones
1.13.3. Ley firma-e, Ley 59/2003, de 19 de diciembre, de firma electrónica

1.14. Normativa europea con implicaciones en protección de datos.

1.14.1. Directiva e-Privacy: Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas) o Reglamento e-Privacy cuando se apruebe.
1.14.2. Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.
1.14.3. Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de

ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

2. Dominio 2. RESPONSABILIDAD ACTIVA.

(Porcentaje temario: 30%)

2.1. Análisis y gestión de riesgos de los tratamientos de datos personales.

2.1.1. Introducción. Marco general de la evaluación y gestión de riesgos. Conceptos generales.

2.1.2. Evaluación de riesgos. Inventario y valoración de activos. Inventario y valoración amenazas. Salvaguardas existentes y valoración de su protección. Riesgo resultante.

2.1.3. Gestión de riesgos. Conceptos. Implementación. Selección y asignación de salvaguardas a amenazas. Valoración de la protección. Riesgo residual, riesgo aceptable y riesgo inasumible.

2.2. Metodologías de análisis y gestión de riesgos.

2.3. Programa de cumplimiento de Protección de Datos y Seguridad en una organización.

2.3.1. El Diseño y la implantación del programa de protección de datos en el contexto de la organización.

2.3.2. Objetivos del programa de cumplimiento.

2.3.3. Accountability: La trazabilidad del modelo de cumplimiento.

2.4. Seguridad de la información.

2.4.1. Marco normativo. Esquema Nacional de Seguridad y directiva NIS: Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Ámbito de aplicación, objetivos, elementos principales, principios básicos y requisitos mínimos.

2.4.2. Ciberseguridad y gobierno de la seguridad de la información. Generalidades, Misión, gobierno efectivo de la Seguridad de la Información (SI). Conceptos de SI. Alcance. Métricas del gobierno de la SI. Estado de la SI. Estrategia de SI.

2.4.3. Puesta en práctica de la seguridad de la información. Seguridad desde el diseño y por defecto. El ciclo de vida de los Sistemas de Información. Integración de la seguridad y la privacidad en el ciclo de vida. El control de calidad de los SI.

2.5. Evaluación de Impacto de Protección de Datos “EIPD”.

2.5.1. Introducción y fundamentos de las EIPD: Origen, concepto y características de las EIPD. Alcance y necesidad. Estándares.

2.5.2. Realización de una evaluación de impacto. Aspectos preparatorios y organizativos, análisis de la necesidad de llevar a cabo la evaluación y consultas previas.

3. Dominio 3. TÉCNICAS PARA GARANTIZAR EL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

(Porcentaje temario: 20%)

3.1. La auditoría de protección de datos.

3.1.1. El proceso de auditoría. Cuestiones generales y aproximación a la auditoría. Características básicas de la Auditoría.

3.1.2. Elaboración del informe de auditoría. Aspectos básicos e importancia del informe de auditoría.

3.1.3. Ejecución y seguimiento de acciones correctoras.

3.2. Auditoría de Sistemas de Información.

3.2.1. La Función de la Auditoría en los Sistemas de Información. Conceptos básicos. Estándares y Directrices de Auditoría de SI.

3.2.2. Control interno y mejora continua. Buenas prácticas. Integración de la auditoria de protección de datos en la auditoria de SI.

3.2.3. Planificación, ejecución y seguimiento.

3.3. La gestión de la seguridad de los tratamientos.

3.3.1. Esquema Nacional de Seguridad, ISO/IEC 27001:2013 (UNE ISO/IEC 27001:2014: Requisitos de Sistemas de Gestión de Seguridad de la Información, SGSI).

3.3.2. Gestión de la Seguridad de los Activos. Seguridad lógica y en los procedimientos. Seguridad aplicada a las TI y a la documentación.

3.3.3. Recuperación de desastres y Continuidad del Negocio. Protección de los activos técnicos y documentales. Planificación y gestión de la Recuperación del Desastres.

3.4. Otros conocimientos.

3.4.1. El cloud computing.

3.4.2. Los Smartphones.

3.4.3. Internet de las cosas (IoT).

3.4.4. Big data y elaboración de perfiles.

3.4.5. Redes sociales

3.4.6. Tecnologías de seguimiento de usuario

3.4.7. Blockchain y últimas tecnologías

ANEXO VI

PROCEDIMIENTO DE SELECCIÓN Y DESIGNACIÓN DE EVALUADORES

El evaluador es el profesional con conocimientos y experiencia profesional equivalente o superior al candidato a certificarse como DPD, y con capacidad para evaluar inicialmente los exámenes, así como las alegaciones que presenten los candidatos durante su realización. Su labor no puede comprometer los principios de independencia e imparcialidad que rigen las tareas de evaluación y de certificación. Se considera que un evaluador cumple las condiciones si está certificado bajo este Esquema AEPD-DPD.

Los evaluadores pueden ser personal propio de la entidad o contratado, en cuyo caso, para cuantas cuestiones puedan surgir respecto al incumplimiento de sus compromisos con relación al Esquema, se ajustarán a lo indicado en el contrato.

El procedimiento de selección define los criterios relativos a la selección y mantenimiento de las empresas o personas contratadas.

1. Requisitos de los evaluadores.

Los evaluadores candidatos deberán cumplir los siguientes requisitos.

a) Titulación universitaria de grado.

b) Experiencia de al menos cinco años en el ámbito de protección de datos y/o de la seguridad de la información.

2. Méritos.

Se valorarán los siguientes méritos:

3.1. Méritos preferentes.

1. Titulación universitaria superior a la de grado: doctorado, posgrado o máster en el ámbito de la protección de datos y/o la seguridad de la información.
2. Experiencia docente en títulos relacionados con la protección de datos o la seguridad de la información.
3. Estar en posesión durante los últimos cinco años de certificaciones relacionadas con la protección de datos o la seguridad de la información.

3.2. Méritos adicionales.

Se valorarán también los siguientes méritos:

1. Experiencia superior a cinco años en el ámbito de protección de datos o seguridad de la información.
2. Participación en comités nacionales o internacionales de normalización relacionados con protección de datos o seguridad de la información.
3. Publicación de artículos relacionados con ambas materias.

3. Incompatibilidades y exclusiones.

Podrán ser excluidos parcial o totalmente del proceso de evaluación aquellas personas que pudieran ver comprometida su independencia e imparcialidad por cualquier circunstancia profesional, familiar o personal.

4. Funciones del evaluador.

El evaluador es responsable de:

1. Evaluar de manera imparcial y confidencial la documentación presentada por los candidatos y las pruebas a que se sometan. La valoración del examen se hará sin conocer la identidad del candidato.
2. Emitir un informe con el resultado de la evaluación.

Además, le corresponde:

1. Informar a la Entidad de Certificación de cualquier relación profesional, familiar o de otro tipo que pueda afectar a la objetividad e imparcialidad de su labor de evaluación.
2. Valorar la recusación motivada de cualquier candidato para su traslado a la Entidad de Certificación.

5. Procedimiento de selección.

La Entidad de Certificación evaluará las candidaturas de los evaluadores y resolverá comunicando su decisión al candidato.

6. Comité de selección.

La Entidad de Certificación creará un órgano interno sujeto a la normativa interna y del Esquema para realizar la selección de los evaluadores.

7. Registros y procedimientos de trabajo.

Se mantendrán archivados los currículums de todos los evaluadores en los que se conserven los registros sobre titulación, formación y experiencia que demuestren su adecuada competencia técnica.

Asimismo, se distribuirán de forma controlada a los evaluadores copias de aquellos documentos del sistema de la calidad que sean de aplicación a su trabajo, y en especial todos los procedimientos y formatos aplicables a la actividad de evaluación.

ANEXO VII

MODELO DE INFORME DEL RESULTADO DE LOS EXÁMENES

El examen queda superado con un resultado igual o superior al 75% de las respuestas correctas, y al menos el 50% en cada uno de los dominios. Sus resultados han sido:

DOMINIO	Puntuación mínima	Puntuación obtenida
1 - Normativa General de Protección de Datos	38	<N1>
2 - Responsabilidad Activa	23	<N2>
3 - Técnicas para Garantizar el Cumplimiento de la Normativa de Protección de Datos y Otros Conocimientos	15	<N3>

PUNTUACIÓN MINIMA PARA SER APTO	113
PUNTUACIÓN OBTENIDA	X
RESULTADO:	APTO/NO APTO

En caso de los no aptos, enviar la información de distribución de errores por epígrafes:

Epígrafes Involucrados	Nº de errores
1.1	
1.2	
1.3	
1.4	
1.5	
1.6	
1.7	
1.9	
1.10	
1.11	
1.14	
2.1	
2.2	

2.3	
2.4	
2.5	
3.1	
3.2	
3.3	
3.4	

ANEXO VIII

CONTENIDO DE LA CERTIFICACIÓN DE CONFORMIDAD CON EL ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS DE DELEGADO DE PROTECCIÓN DE DATOS

Cada Entidad Certificadora podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema de la AEPD de Delegado de Protección de Datos, que deberá mostrar, al menos, el contenido siguiente:

— Logotipo de la Entidad Certificadora.

— Identificación de la Entidad Certificadora.

— Marca del Esquema de Certificación de Delegados de Protección de Datos

— Texto: "Certificado de Conformidad con el Esquema de Certificación de Delegado de Protección de Datos de la Agencia Española de Protección de Datos".

— Texto: "«Entidad Certificadora» certifica que el candidato reseñado, ha sido evaluado y encontrado conforme con las exigencias del Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos:"

— «identificar con nombre, apellidos y DNI a la persona objeto de la certificación».

— Texto: "Número de certificado: «número de certificado»".

— Texto: "Fecha de certificación de conformidad inicial: «día» de «mes» de «año»'.

— Texto: "Fecha de renovación de la certificación de conformidad: «día» de «mes» de «año»".

— Texto: "Fecha de caducidad de la certificación de conformidad: «día» de «mes» de «año»".

— Texto: "Fecha: «Localidad (la que corresponda)», «día» de «mes» de «año»".

— Firma: Nombre y Apellidos del responsable competente de la Entidad Certificadora.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la certificación expedida.

A continuación, se muestra un modelo ilustrativo de la citada Certificación de conformidad.

Logotipo de la Entidad Certificadora con marca de acreditación	MARCA DEL ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS

Certificación de Conformidad con el Esquema de la Agencia Española de Protección de Datos de Delegado de Protección de Datos

Entidad Certificadora podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema de la AEPD de Delegado de Protección de Datos, que deberá mostrar, al menos, el contenido siguiente:

— Logotipo de la Entidad Certificadora.

— Identificación de la Entidad Certificadora.

— Marca del Esquema de Certificación de Delegados de Protección de Datos

— Texto: "Certificado de Conformidad con el Esquema de Certificación de Delegado de Protección de Datos de la Agencia Española de Protección de Datos".

«Entidad Certificadora» certifica que el candidato reseñado, ha sido evaluado y encontrado conforme con las exigencias del Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos, según se indica en el correspondiente Informe de Certificación de «fecha» para:

«identificar con nombre, apellidos y DNI a la persona objeto de la certificación».

"Fecha de certificación de conformidad inicial: «día» de «mes» de «año»

"Fecha de renovación de la certificación de conformidad: «día» de «mes» de «año»"

"Número de certificado: «número de certificado»

"Fecha: «Localidad (la que corresponda)», «día» de «mes» de «año»

Firma: «Nombre y Apellidos del responsable competente de la Entidad Certificadora»

Firma del responsable de la Entidad Certificadora

Nombre completo/razón social de la Entidad Certificadora y página web.

Dirección postal/electrónica

Código Postal, Provincia, País.

ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD).

aepd agencia española protección datos