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

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

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

Redactado por la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos
2 de octubre 2017. Versión 1.1

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Índice

1. OBJETO

El objeto de este documento es establecer las líneas generales que regulan el funcionamiento del Esquema de Certificación de Personas para la categoría de "Delegado de Protección de Datos" (en adelante, DPD) 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 estarán implicados en dicha certificación bajo condiciones de acreditación.

La certificación de personas es una herramienta 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 a las personas para obtener la certificación profesional. La validez y vigencia de las reglas del Esquema se asegura a través de la involucración 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 de su actuación sistemática e imparcial, se consigue 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), 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 de Certificación de 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 de protección de datos de carácter personal.
- Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal.

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
- LOPD: Ley Orgánica de protección de datos de carácter personal
- RLOPD: Reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter personal.

2. AGENTES DEL ESQUEMA

- **La AEPD** como propietario 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).** Es 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 a 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 personas certificadas, en los términos establecidos en el apartado 3.

Dicha autorización de la AEPD a una Entidad de Certificación, estará condicionada a la obtención inicial y al mantenimiento de la acreditación, pudiendo ser rescindida si:

- ENAC retira a la EC la acreditación para actuar en este Esquema.
- La EC incumple las reglas de uso de marcas o no cumple con su obligación de vigilancia del uso de estas por parte de las personas por ella certificadas.
- La EC incurre en cualquier otro incumplimiento de las reglas establecidas por la AEPD.

- **Las Entidades de Formación (EF).** Son las entidades que ofertan una formación que satisfaga los requisitos previos de la certificación a este respecto. La AEPD podrá establecer, en su caso, un proceso público y no discriminatorio de autorización de EF. Si fuera preciso, se publicarán los requisitos de reconocimiento exigibles tanto a los programas de formación como a las entidades impartidoras de los mismos 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 Entidades de Formación deberán solicitar a las Entidades de Certificación el reconocimiento de sus programas de formación siguiendo los requisitos establecidos en el apartado 6.3.

3. MARCA DEL ESQUEMA

La AEPD, al objeto de que el mercado sea capaz de identificar a los Delegados de Protección de Datos certificados según el Esquema propiedad de la AEPD, ha creado una Marca de conformidad con el Esquema (en adelante, la Marca del Esquema). La AEPD podrá ceder a cualquiera de los agentes del Esquema los derechos de su uso de la misma de acuerdo a unas normas específicas

En el **Anexo II.A** se adjuntan las normas de uso de la marca y en el **Anexo II.B** el modelo de contrato de uso de marca.

Los agentes identificados en el apartado 2 podrán hacer uso exclusivamente de la Marca del Esquema para indicar tal condición, una vez recibida la autorización por la AEPD y mientras se mantenga vigente tal autorización. Se ajustarán en todo momento a las reglas de uso de la Marca que les afecten.

Cualquier uso o cesión de uso de la Marca del Esquema, así como las limitaciones del mismo, se regularán a través de referencias concretas en los “contratos” que en cada caso se establezcan entre la AEPD y el agente.

4. COMITÉ DEL ESQUEMA

La AEPD se responsabiliza del desarrollo, revisión y validación periódica del Esquema de certificación de DPD, al menos cada cinco años, pudiéndose revisar antes si las condiciones de cambio lo aconsejan. Para ello, ha creado y mantiene un Comité del Esquema de certificación de DPD (en adelante, el Comité del Esquema), 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, además de la AEPD como propietario del mismo y por entidades, organizaciones y asociaciones interesadas.

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

5. AUTORIZACIÓN DE LAS ENTIDADES DE CERTIFICACIÓN

El reconocimiento o designación de aquellas entidades de certificación que puedan ofrecer y llevar a cabo la certificación de personas de acuerdo con Esquema AEPD-DPD se basa en los criterios y requisitos establecidos por él.

Tal reconocimiento se basa, pero no se limita, en la competencia técnica para certificar, para lo cual requieren la obtención y el mantenimiento de la acreditación por ENAC para la certificación de personas como Delegados de Protección de datos bajo el Esquema de la Agencia (Esquema AEPD-DPD).

La participación de ENAC, proporcionando la acreditación, asegura que la designación de entidades de certificación se limite exclusivamente a aquellas que hayan demostrado su competencia técnica para esta actividad en particular, de acuerdo con criterios internacionalmente aceptados.

A demás, la designación por parte de la AEPD está dirigida estrictamente a informar a las personas potencialmente interesadas en certificarse como “Delegados de Protección de Datos” sobre las entidades que realizan la certificación de acuerdo con los requisitos definidos por la AEPD y su Comité del Esquema.

La AEPD mantendrá un registro actualizado de las entidades de certificación autorizadas, que incluirá los siguientes datos suministrados por ENAC: nombre, número de autorización, fecha de concesión.

Las entidades de certificación autorizadas son responsables de comunicar a la AEPD cualquier cambio significativo en su condición de acreditados, como la suspensión o retirada de la acreditación por ENAC, que pueda afectar a los requisitos de reconocimiento.

La AEPD verificará que se cumplen continuamente las obligaciones derivadas del reconocimiento y del uso de la Marca de Conformidad, ya sea a través de actuaciones propias o a través de la información que puedan aportar las personas certificadas y las empresas usuarias finales de la certificación de "Delegado de Protección de Datos".

Con objeto de facilitar la adquisición de experiencia en el Esquema, las entidades de certificación podrán solicitar y ser objeto de una designación provisional, no renovable y con una vigencia máxima de un año. Esta autorización provisional estará condicionada a la presentación de la solicitud de la acreditación a ENAC y a la superación favorable de la fase de revisión de la solicitud. Durante este primer año de designación provisional, se deberán haber realizado, al menos, dos convocatorias del examen de certificación.

Durante la validez de la designación provisional, la entidad de certificación podrá, con el único propósito de facilitar el acceso a la certificación a las personas interesadas y así adquirir la necesaria experiencia, hacer uso de la condición de entidad de certificación designada provisionalmente por el Esquema; sin embargo, no podrá hacer uso alguno de las marcas del Esquema (de ENAC y de la AEPD). Si, transcurrido un año desde la designación provisional, la entidad de certificación no ha conseguido la acreditación por ENAC, siempre que sea por razones imputables a la entidad de certificación, aquella se extinguirá automáticamente.

6. ESQUEMA 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 puede emitir una declaración de cumplimiento o certificado.

6.1. PERFIL DEL PUESTO DE DELEGADO DE PROTECCIÓN DE DATOS.

El DPD es un profesional cuyas funciones se señalan en el artículo 39 del Reglamento (UE) 679/2016, y se ocupa de la aplicación de la legislación sobre privacidad y protección de datos.

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
b) supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los 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 la evaluación de impacto relativa a la protección de datos
g) supervisar su aplicación de conformidad con el artículo 35 del Reglamento;
h) cooperar con la autoridad de control;
i) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y
j) realizar consultas a la autoridad de control, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos 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 información para determinar las actividades de tratamiento,
b) analizar y comprobar la conformidad de las actividades de tratamiento, e
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
    - 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 con 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 (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con el Reglamento.

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos.

h) asesorar al responsable del tratamiento sobre:
   - qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos,
   - qué áreas deben someterse a auditoría de protección de datos interna o externa,
   - qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

6.2. 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 o destrezas necesarias que tiene que saber o poseer la persona a certificar para llevar a cabo cada una de las funciones propias del puesto de Delegado de Protección de Datos.

Estas 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 determinar 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 mecanismos 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 de transferencia internacional 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 riesgo 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.

6.3. 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 en materia de protección de datos.

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

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

El reconocimiento de los programas de formación se hará de acuerdo con varios requisitos: duración requerida, 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) y la metodología didáctica que incluya impartición de conocimientos teóricos, realización de ejercicios prácticos y desarrollo de ejercicios en grupo.

La distribución de las horas de los programas de formación seguirá el mismo porcentaje establecido para cada uno de los dominios del programa del Esquema.

Las entidades de formación solicitarán a las de certificación el reconocimiento de los programas de formación que imparten de acuerdo con los requisitos arriba mencionados.

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

Se valorará la formación y experiencia adquiridas a escaka nacional y en la Unión Europea.

La valoración de la formación y experiencia exigidas en los prerrequisitos relativa al Reglamento General de Protección de Datos (RGPD) será la adquirida a partir de la fecha de entrada en vigor del citado reglamento: 25/5/2016.

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

6.4. CÓDIGO ÉTICO.

A efectos de justificar cuestiones como la integridad y un elevado nivel de ética profesional que debe cumplir el candidato a DPD, se ha plasmado en un documento que recoge este compromiso, cuyo contenido se detalla en el **Anexo III**.

El Código Ético debe ser aceptado por el solicitante previamente a la concesión del certificado.

6.5. 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 tareas correspondientes a la actividad de Delegado de Protección de Datos, en los términos y condiciones establecidas por el Esquema de certificación de la AEPD.

6.5.1. 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 las correspondientes tareas 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 solicitante para realizar funciones de Delegado de Protección de Datos.
- El examen engloba una prueba que consta de 150 preguntas tipo test de respuesta múltiple, siendo necesario para su aprobación haber superado el 75%. 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.
- Dominio 2 – 30%, 45 preguntas, de ellas 9 con escenario.
- Dominio 3 – 20%, 30 preguntas, de ellas 6 con escenario.

- Para la aprobación de la prueba, se requiere haber respondido correctamente al 50% de las preguntas 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 es incorrecta o se deja en blanco. Se requiere, pues, para su aprobación haber obtenido, al menos, 112,5 puntos.
- 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 tres meses.
- Ello sin perjuicio de que, mediante acuerdo de todas las entidades de certificación, se puedan establecer convocatorias únicas y coordinadas.

6.5.2. 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 GT art.29, etc.

Ponderación: 50%.

Dominio 2 RESPONSABILIDAD ACTIVA. Evaluación y gestión de riesgos de 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 IV**.

6.5.3. Evaluadores

El grupo de evaluadores está constituido por profesionales independientes del Esquema con formación y experiencia profesional equivalente o superior al candidato a certificar, con capacidad de evaluar las pruebas del método de evaluación. Han de garantizar la independencia de criterio, emitiendo un informe con el resultado de la evaluación en el cual se basa la decisión de concesión del certificado al candidato evaluado.

Los evaluadores que participan en el proceso de evaluación deberán haber sido designados de acuerdo con el proceso y requisitos descritos en el **Anexo V**. En este documento se detallan también las actividades de supervisión de la actuación de los evaluadores establecidas por el Esquema.

6.6. CRITERIOS PARA LA CERTIFICACIÓN.

6.6.1. Certificación inicial.

Para obtener la certificación como DPD, los candidatos deberán cumplir con los prerrequisitos establecidos en el apartado 6.3 y presentar la siguiente documentación:

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 someterse a las pruebas de evaluación.

Una vez presentada la solicitud, la Entidad de Certificación procederá a su evaluación para comprobar que toda la información está completa.

Si, tras dicha evaluación inicial, la información no estuviera completa, se informará al candidato de la no aceptación de la solicitud de certificación mediante notificación

escrita. Se dará un plazo de 10 días hábiles para que pueda subsanar. Si, transcurrido dicho plazo, no fuera posible subsanar la deficiencia notificada, se declarará al candidato como no admitido, lo que se le comunicará mediante notificación escrita.

Si la solicitud es aceptada, se informará al candidato mediante notificación escrita.

La aceptación de la solicitud supondrá la admisión en la convocatoria a la prueba de evaluación.

Si la solicitud es aceptada, pero no para la fecha de convocatoria deseada, en caso de existir varias convocatorias, el solicitante también será notificado por escrito.

Cualesquiera decisiones de la Entidad de Certificación respecto al proceso de aceptación podrán ser objeto de la correspondiente reclamación en los términos establecidos en el apartado 7 del presente Esquema.

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

El solicitante deberá presentarse para verificar su identidad y superar el examen.

En todos los casos en los que se suspenda la prueba de evaluación, se informará por escrito al solicitante del resultado, previamente a la realización del nuevo examen, en el caso de que tenga derecho a repetición.

6.6.2. Concesión del certificado.

Tras superar el examen, la Entidad de Certificación concederá la certificación a los candidatos que hubieran obtenido el resultado de “apto”.

Previamente el solicitante deberá aceptar expresamente el Código Ético y las Normas de Uso de la marca del certificado.

A cada persona certificada la Entidad de Certificación le asignará un número identificativo intransferible y que será utilizado en el futuro para su identificación, junto con el número identificativo de la entidad de certificación que emitió el certificado.

En los casos en que se conceda la certificación, la Entidad de Certificación emitirá un certificado justificativo que será enviado al titular de la certificación, de acuerdo con el **Anexo VI**.

El certificado emitido tendrá un período de validez de tres años, salvo que la persona certificada sea sancionada. El período de validez comenzará a partir de la fecha de concesión del certificado.

6.6.3. 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.

6.6.4. Renovación de la Certificación.

La certificación tendrá un periodo de validez de tres años y su renovación 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 en materia de protección de datos de carácter personal 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. No será valorada la formación en la que no conste su duración, el temario, la entidad de formación y el título de la formación. En el caso excepcional y justificado de no 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.

La renovación habrá de solicitarse con anterioridad a la fecha de vencimiento del periodo de validez del certificado.

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

La no recepción por la persona certificada de la comunicación de la Entidad de Certificación 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 junto con la relación de las reclamaciones que, en su caso, haya podido tener durante el período completo de duración de la certificación por actuaciones defectuosas en la actividad propia para la que esté certificado o una declaración en la que haga constar que no ha sido objeto de ninguna reclamación. Deberá acompañar la aceptación del Código Ético y las Normas de

Uso de la marca del certificado y el Contrato de Cesión de Uso, además de la justificación del pago de las tasas de renovación.

Una vez presentada la solicitud, la Entidad de Certificación procederá a la evaluación de la misma para la comprobación de la validez de toda la documentación proporcionada. Si tras dicha evaluación inicial, la información no estuviera completa, se informará al candidato de la no aceptación de la solicitud de renovación mediante notificación escrita. Se dará un plazo máximo de 90 días naturales para que pueda subsanar. Si, transcurrido dicho plazo, no fuera posible subsanar la deficiencia notificada, se declarará al candidato como no renovado, lo que se le comunicará mediante notificación escrita y se procederá a la retirada del certificado.

Si la solicitud es aceptada, se informará al candidato mediante notificación escrita.

En el caso en que se renueve la certificación, la Entidad de Certificación emitirá un nuevo certificado justificativo con el mismo número identificativo asignado en la primera certificación. El nuevo certificado tendrá un periodo de validez de tres años.

6.7. CRITERIOS PARA LA SUSPENSIÓN O RETIRADA DE LA CERTIFICACIÓN.

6.7.1. Suspensión temporal voluntaria.

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

Para la vuelta a la condición de certificado, la entidad de certificación requerirá realizar comprobaciones encaminadas a confirmar 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 que justifique documentalmente que está en condiciones de obtener el certificado, en los mismos términos establecidos para la renovación en el apartado anterior.

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

6.7.2. Suspensión temporal por conductas contrarias al Esquema.

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

- La no presentación por parte de la persona certificada de documentación, registros o cualquier información que le haya sido requerida por la entidad de certificación para mantener dicha certificación o para investigar una reclamación dirigida a la persona.

- 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 las marcas de certificación de manera no permitida o contraria a las reglas de uso de marcas del Esquema.

- 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 mínimo de seis meses hasta la mitad del ciclo de certificación, superada la cual se procederá a la retirada de la certificación.

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

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

Para la vuelta a la condición de certificado, la entidad de certificación deberá requerir las oportunas comprobaciones para confirmar que las causas que motivaron la suspensión han desaparecido, pudiéndose llegar incluso a exigir una reevaluación parcial o total.

6.7.3. Retirada de la certificación.

Serán motivos que deberán llevar a una entidad de certificación a la retirada de una certificación ya emitida, los siguientes:

- Cualquiera de las identificadas anteriormente para la suspensión temporal, en función de su gravedad o su reiteración, como la reiteración en un tipo concreto de incumplimiento que ya motivó una suspensión temporal, lo que implica que no se ha corregido la conducta del DPD.
- La suspensión de la certificación por un periodo superior a la mitad del ciclo de certificación.
- La falta de colaboración de la persona certificada para la devolución del certificado en caso de sanción.

Para la vuelta a la condición de certificado, la persona afectada deberá someterse a un proceso de certificación inicial completo. La Entidad de Certificación podrá requerir a la persona que, previamente a someterse a la evaluación, evidencie haber resuelto las causas que llevaron a la retirada del certificado anterior sin que ello pueda ser considerado como trato discriminatorio.

La Entidad de Certificación se reservará el derecho a aceptar una nueva solicitud por parte del profesional sancionado.

6.8. DERECHOS Y OBLIGACIONES DE LAS PERSONAS CERTIFICADAS.

6.8.1. 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.
- Reclamar y a recurrir cualquier decisión desfavorable.

6.8.2. 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 y la marca del Esquema para usos 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 las entidades de certificación.
- No tomar parte en prácticas fraudulentas relativas a la sustracción y/o divulgación del material del 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 podrá suponer el inicio del proceso de suspensión o retirada del certificado.

6.9. INFORMACIÓN SOBRE PERSONAS CERTIFICADAS.

Las Entidades de Certificación mantendrán actualizado, como mínimo semestralmente, un registro público del estado en vigor de las personas certificadas. Este listado contendrá, como mínimo, nombre y apellidos, número de certificado, fecha de concesión, fecha de caducidad y estado del certificado (concedido, suspendido, retirado, renovado), y estará disponible para cualquier persona interesada.

7. GESTIÓN DE QUEJAS Y RECLAMACIONES SOBRE EL ESQUEMA

7.1. ÁMBITO DE APLICACIÓN.

Podrán ser objeto de queja o reclamación cualesquiera actuaciones contrarias al Esquema realizadas por los Agentes y por las personas certificadas con arreglo al mismo. Serán objeto

de especial atención las conductas de los Delegados de Protección de Datos certificados que resulten contrarias al Código Ético del Esquema.

7.2. 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 al Agente correspondiente que haya realizado la declaración pública que sea objeto de reclamación, antes de dirigirla a la AEPD.

Cualquier queja o reclamación, bien a la AEPD, bien a ENAC o a una EC autorizada, por parte de un tercero, relativa a la actuación o desempeño de una persona certificada en el Esquema, deberá ser reenviada al resto de agentes y gestionada en primera instancia por la EC autorizada que la haya certificado. Las responsabilidades dependerán del contenido de dicha reclamación.

Si la reclamación es relativa a una persona certificada o a la actuación de la EC, la citada queja o reclamación deberá ser gestionada por ésta de acuerdo a lo requerido por la norma UNE-EN ISO/IEC 17024. El tratamiento dado a las mismas, así como su resolución, serán verificadas por ENAC como parte de su evaluación.

Si la reclamación está relacionada con la acreditación concedida, deberá ser gestionada por ENAC, quien además deberá tramitar aquellas reclamaciones o quejas que procedan de reclamantes insatisfechos con la respuesta dada, en primera instancia, por una EC autorizada y, por lo tanto, acreditada.

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 tratada por las instancias anteriores.

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 con la instancia anterior (EC o ENAC). La AEPD

adoptará la resolución correspondiente una vez oído al Comité del Esquema. La AEPD notificará al reclamante de la decisión tomada al respecto.

7.3. PROCEDIMIENTO DE QUEJAS Y RECLAMACIONES.

El proceso para el tratamiento y resolución de las quejas o reclamaciones será el establecido por la correspondiente Entidad de Certificación conforme a la norma UNE-EN ISO/IEC 17024, que en todo caso 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 evaluación 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 contemplando 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 reclamación y/o quejas.

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

c) Proporcionar a los clientes un formulario para rellenar en caso de cualquier queja relacionada con los servicios prestados, que se remitirá tanto a la persona certificada y Organización afectada por la queja, 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.

8. 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 del funcionamiento del mismo, especialmente durante las primeras etapas de su aplicación.

ANEXOS

Anexo I. Condiciones de justificación de los prerrequisitos.

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 entre la AEPD y los Agentes del Esquema.

Anexo III. Código Ético.

Anexo IV. Programa (temario) del Esquema.

Anexo V. Procedimiento de selección y designación de evaluadores.

Anexo VI. Modelo de documento justificativo de la certificación

ANEXO I
CONDICIONES DE JUSTIFICACIÓN DE LOS PRERREQUISITOS

A. FORMACIÓN.

- Aportar certificado de haber recibido una formación mínima reconocida, en relación con las materias objeto del programa del Esquema.
- Justificar, según los prerrequisitos, una formación de 60, 100 o 180 horas.
- El reconocimiento de la formación se hará según los requisitos definidos en el Esquema, por las Entidades de Certificación.
- La distribución de las horas de los programas de formación seguirá el mismo 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 son 25 horas y 1 LRU son 10 horas.

B. EXPERIENCIA LABORAL O PROFESIONAL.

Justificar la experiencia laboral o profesional requerida por los prerrequisitos: dos, tres o cinco años de experiencia. Para ello deberá aportarse evidencia objetiva de la experiencia general y específica mediante declaración del empleador o cliente, contrato de trabajo, etc.

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

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 de riesgo no alto.

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

Solo 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 como el doble de horas de la formación recibida.

Para la formación impartida en una materia específica solo 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 ptos.	300 ptos.
60 horas	3 años	60 ptos.	180 ptos.
100 horas	2 años	60 ptos.	120 ptos.
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. Tan solo 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
		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.	10	Superación de trabajo fin de curso con una dedicación de al menos 40 horas.	1,5	5
Prácticas en empresas en temas de protección de datos o privacidad.	10	Realización de prácticas en empresas con una dedicación de al menos 40 horas.	1,5	5
Experiencia laboral en temas de protección de datos o privacidad.	50[5]	Funciones específicas de privacidad del puesto de trabajo, por año de experiencia	10	30
		Profesional o asalariado que realiza actividades diversas, por proyecto (se valorará complejidad, duración y papel desempeñado)	5	20

[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.
[5] Experiencia diferente de la utilizada para la valoración como prerrequisito.

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.	5	Premios y reconocimientos profesionales o similar.	5	10
Certificaciones en materias de protección de datos o privacidad (en vigor).	5	ACP-DPO de APEP, CDPP de ISMS FORUM[6], ECPC-B DPO de Universidad de Maastricht, DPO de EIPA (European Institute of Public Administration) o similar.	4	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[7], 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

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

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 Agentes del esquema de certificación para hacer público este hecho.

La Marca del Esquema se utilizará exclusivamente por la AEPD, las entidades de certificación autorizadas, ENAC y las agencias/academias de formación homologadas.

El diseño y las características que conforman la Marca del Esquema se especifican en el Anexo del presente documento.

2. USOS.

La Marca del Esquema se utilizará exclusivamente para indicar que el agente en cuestión está autorizado por la AEPD como agente involucrado en el desarrollo del esquema.

No podrá ser usada por personas físicas, independientemente de que se encuentren certificadas o no como DPO de acuerdo a las reglas del esquema.

Tampoco podrá ser empleada por ningún agente durante el periodo en el que dure su autorización provisional y hasta tanto no obtenga la correspondiente acreditación por ENAC.

3. REGLAS DE USO.

Serán condiciones de uso de la Marca del Esquema, las siguientes:

a) Sólo podrá ser utilizada por los agentes a posteriori de haber sido expresamente autorizados por la AEPD para ello, en relación con la certificación de "Delegado de Protección de Datos".

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

c) El agente podrá emplearla en documentos o soportes de tipo publicitario (folletos, páginas web, etc.), de forma que quede clara su vinculación únicamente con el servicio de certificación de personas como “Delegado de Protección de Datos” de la AEPD, y no con cualquier otro servicio similar que se oferte al mercado.

d) No está permitido el uso de la Marca del Esquema en cualquiera de sus formas (por ej., en las tarjetas de visita), por parte de personas integrantes, trabajadores o colaboradores de cualquiera de los agentes autorizados, incluidas aquellas de la AEPD o vocales del Comité del esquema.

e) El agente debe dejar de emplear la Marca del Esquema en el caso de una suspensión de la autorización durante el periodo de la misma, así como de forma permanente cuando haya perdido su condición de autorizado, ya sea debido a una baja voluntaria, a la retirada de la acreditación ENAC (en el caso de las entidades de certificación) o a otro motivo.

ANEXO

Marca a determinar por la Agencia posteriormente.

ANEXO II.B
MODELO DE CONTRATO DE USO DE LA MARCA DEL ESQUEMA ENTRE LA AEPD Y LOS AGENTES DEL ESQUEMA

CLÁUSULA PRIMERA. 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 el Esquema de la AEPD, se crea la Marca del Esquema, que será el símbolo usado por los Agentes del Esquema de Certificación AEPD-DPD para hacer público este hecho.

Esta marca se utilizará exclusivamente por la AEPD, las Entidades de Certificación autorizadas, ENAC y, en su caso, las Entidades de Formación homologadas.

El diseño y las características de la Marca del Esquema son las establecidas en el Anexo de las Normas de Uso de la Marca del Esquema AEPD-DPD.

CLÁUSULA SEGUNDA. USOS.

La Marca del Esquema se utilizará exclusivamente para indicar que el agente en cuestión está autorizado por la AEPD como agente involucrado en el desarrollo del Esquema.

No podrá ser usada por personas físicas, independientemente de que se encuentren certificadas o no como DPD de acuerdo a las reglas del Esquema.

No podrá ser empleada por ningún agente en el periodo en el que dure su autorización provisional, y hasta tanto no obtenga la correspondiente acreditación por parte de ENAC.

CLÁUSULA TERCERA. REGLAS DE USO.

El uso de la Marca del Esquema se sujetará a las siguientes reglas:

a) Sólo podrá ser utilizada por los agentes a posteriori de haber sido expresamente autorizados por AEPD para ello, en relación con la certificación de "Delegado de Protección de Datos".

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

c) El Agente podrá emplear la Marca del Esquema en documentos o soportes de tipo publicitario (folletos, páginas web, etc.), de forma que quede clara su vinculación únicamente

con el servicio de certificación de personas como “Delegado de Protección de Datos” de la AEPD y no con cualquier otro servicio similar que se oferte al mercado.

d) El Agente debe dejar de emplear la Marca del Esquema en el caso de una suspensión de la autorización durante el periodo de la misma, así como de forma permanente cuando haya perdido su condición de autorizado, ya sea debido a una baja voluntaria, a la retirada de la acreditación ENAC (en el caso de las entidades de certificación) o a otro motivo.

e) No está autorizado el uso de la Marca del Esquema en cualquiera de sus formas (por ejemplo, en las tarjetas de visita), por parte de personas integrantes, trabajadores o colaboradores de cualquiera de los Agentes autorizados, incluidas aquellas de la AEPD o vocales del Comité del Esquema.

ANEXO III
CODIGO ETICO 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 contenidos en el mismo, 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 éste 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 pueda 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 interés 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 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 espacio 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 interés 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 rellenar en caso de 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 él, 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 IV
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 actualización de LOPD. 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 actualización de 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 actualización de LOPD. 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 actualización de LOPD. 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 actualización de LOPD. 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 actualización de LOPD. 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 actualización de LOPD. Las 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 V
PROCEDIMIENTO DE SELECCIÓN Y DESIGNACION DE EVALUADORES

Los evaluadores pueden ser personal propio de la entidad o personal subcontratado (autónomos o por cuenta ajena).

Para cuantas cuestiones puedan surgir respecto al incumplimiento de sus compromisos con relación al Esquema, se ajustarán a lo indicado en el contrato.

Este procedimiento define los criterios relativos a los procesos de selección y mantenimiento de las empresas o personas subcontratadas.

1. Registros y procedimientos de trabajo.

Se mantendrán archivados los curricula 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.

2. 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 o de la seguridad de la información.

3. 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 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.

4. Incompatibilidades y exclusiones.

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

5. 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.

6. Procedimiento de selección.

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

7. 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.

ANEXO VI
CONTENIDO DE LA CERTIFICACION DE CONFORMIDAD CON EL ESQUEMA DE LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS DE DELEGADO DE PROTECCION 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.

— Logotipo 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

LOGOTIPO 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.

— Logotipo 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).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS