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).

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»

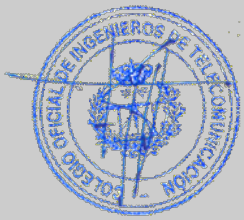
Firma del responsable de la Entidad Certificadora

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