ISMS Forum Spain

ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN

Certified Data Privacy Professional (CDPP)

Temario del examen de certificación

DPI Data Privacy Institute

AN ISMS FORUM INITIATIVE

Índice

0. INTRODUCCIÓN AL CDPP

ISMS Forum Spain a través del Data Privacy Institute, ha creado la primera certificación española en el ámbito de la Privacidad y la Protección de datos de carácter personal: **Certified Data Privacy Professional (CDPP)**.

La obtención de esta certificación acredita un alto nivel de especialización en la normativa española en materia de Protección de datos de carácter personal, tanto en un contexto local, como en un contexto europeo e internacional, así como un dominio de los fundamentos que rigen la Seguridad de la Información.

Para obtener la certificación CDPP, los candidatos deberán cumplir con los siguientes requisitos:

1. **Aprobar el Examen de Certificación CDPP**

El examen se compone de 150 preguntas de selección múltiple, que abarcan la comprensión de siete dominios de conocimiento sobre la Privacidad y la Protección de datos de carácter personal, y sobre la Seguridad de la Información. Así mismo, cuenta con un caso práctico relacionado con estos dominios en el que se plantean 20 alternativas con las opciones: Verdadero/Falso. Éste examen se aprueba con un 75% de respuestas correctas y con arreglo a la siguiente ponderación:

1. Dominio-1: Fundamentos de la Protección de Datos (5%)
2. Dominio-2: Marco normativo general de la Protección de Datos en España (22%)
3. Dominio-3: Marco normativo sectorial de la Protección de Datos en España (18%)
4. Dominio-4: Marco normativo internacional y de la unión europea de la Privacidad y Protección de datos (10%)
5. Dominio-5: Protección de los Activos de Información (15%)
6. Dominio-6: Gestión y Respuesta ante Incidentes (10%)
7. Dominio-7: Control y Auditoría de los Sistemas de Información (20%)

2. **Acreditar que cuenta con al menos, tres años de experiencia en el ámbito de la Privacidad y la Protección de datos**

Los candidatos que hayan aprobado el examen serán requeridos para acreditar esta experiencia. En caso de que el candidato no cuente con esta experiencia, o que la misma no pueda ser acreditada, los resultados de aprobación examen serán válidos por tres años.

1. DOMINIO 1: FUNDAMENTOS DE LA PROTECCIÓN DE DATOS

1.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga conocimientos suficientes sobre la evolución en España de un derecho fundamental recogido en la Constitución Española: El denominado derecho a la intimidad. Así mismo, se pretende que el candidato conozca los fundamentos relativos al reconocimiento de la protección de datos como un derecho fundamental autónomo e independiente, por parte de Tribunal Constitucional.

Adicionalmente, se pretende evaluar el conocimiento de la más importante normativa en materia de protección de datos de carácter personal en el ámbito comunitario. En particular, se pretende que el candidato demuestre un conocimiento suficiente de los principios consagrados en los principales textos normativos existentes en el ámbito europeo.

1.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Disponer de un conocimiento suficiente sobre la evolución de la normativa de protección de datos en el ámbito comunitario desde 1950 hasta la actualidad y en especial, de los principios esenciales consagrados en la misma a lo largo del tiempo.
2. Obtener un conocimiento suficiente sobre la evolución de la normativa española de protección de datos, y de sus principios fundamentales.
3. Disponer de criterios suficientes para determinar la necesidad de conexión entre la normativa española, la comunitaria, y la internacional.
4. Adquirir un conocimiento suficiente de la Doctrina y la Jurisprudencia más relevante, en relación con los aspectos antes mencionados.

1.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Marco Europeo de desarrollo de los derechos y libertades de las personas:
   a) Convenio Europeo por la protección de los Derechos humanos y libertades fundamentales de 4 de noviembre de 1950: Art. 8.1.
   b) Convenio 108 del Consejo de Europa, de 28 de enero de 1981.
   c) Protocolo adicional del Convenio nº 108, de 8 de noviembre de 2001.
   d) Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos: importancia del considerando 27.
   e) Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones.
   f) Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (Directiva que deroga la anterior).
   g) Directiva 2006/24/CE, sobre conservación de datos guardados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
   h) Reglamento 45/2001/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios a la libre circulación de estos datos.

2. Marco Español de desarrollo del derecho fundamental a la protección de datos de carácter personal:
   a) Artículos 18.1 y 18.4 de la Constitución Española.
   b) La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), similitudes y diferencias con LOPD. Desarrollos reglamentarios de dichas normas: Real Decreto 1332/1994, de 20 de Junio y Real Decreto 1720/2007 de 21 de diciembre.
   c) La evolución en el marco del Tribunal Constitucional: Las sentencias 290 y 292/2000 de 30 de noviembre: Los preceptos de la Ley Orgánica 5/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) declarados inconstitucionales.
   d) Importancia de las Sentencias del Tribunal Supremo. Sentencias de la Sala de lo Contencioso-Administrativo del Tribunal Supremo de fecha 15 de julio

de 2010 (Recursos 23/2008, 25/2008 y 26/2008) que resuelve sobre la nulidad de determinados artículos del Reglamento de desarrollo de la LOPD.

e) Modificaciones introducidas por la Ley 2/2011, de 4 de marzo, de Economía Sostenible (Ley "Sinde"). Modificación del Régimen Sancionador de la LOPD y novedad de la figura de apercibimiento
f) La LOPD: Principales novedades en cuanto a obligaciones, responsabilidades, figuras jurídicas.

2. DOMINIO 2: MARCO GENERAL DE LA PROTECCIÓN DE DATOS EN ESPAÑA

2.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga conocimientos suficientes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de desarrollo (en adelante RLOPD o Reglamento de desarrollo), así como la capacidad de aplicar sus disposiciones en cualquier tipo de organizaciones sea ya sean estas de ámbito público o privado.

2.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son la identificación de necesidades jurídicas y organizativas de cumplimiento normativo en materia de protección de datos personales existentes en cualquier entidad. En particular:

1. Obtener la capacidad suficiente para aplicar los principios que rigen el tratamiento de datos de carácter personal y de diseñar con arreglo a ellos, una estrategia adecuada en cuanto a privacidad y protección de datos personales.
2. Conocer las obligaciones que recaen sobre las organizaciones como responsables de fichero.
3. Definir las diferentes figuras que se dan en el ámbito de la protección de datos dentro de la organización y sus funciones.
4. Disponer de la capacidad para planificar la salvaguarda de los derechos de los titulares de los datos personales por parte de la organización.
5. Contar con la capacidad suficiente para gestionar los distintos procedimientos iniciados por cualquiera de las agencias de protección de datos.

2.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Principios y figuras jurídicas consagradas por la LOPD y desarrollados por el RLOPD:

a) Calidad de los datos.
b) Derecho de información en la recogida de datos.
c) Consentimiento del afectado.
d) Datos especialmente protegidos.
e) Datos relativos a la salud.
f) Seguridad de los datos.
g) Deber de secreto.
h) Comunicación de datos.
i) Acceso a los datos por cuenta de terceros.
j) Responsable del fichero.
k) Encargado del tratamiento.
l) Responsable de seguridad.
m) Cesionarios y cedente.
n) Transferencias internacionales de datos.
o) Importador y exportador de datos.
p) Otras.

2. Principales obligaciones en materia de protección obligaciones que recaen sobre las organizaciones como responsables de fichero:
   a) Inscripción de ficheros.
   b) Documento de seguridad.
   c) Nombramiento del responsable de seguridad.
   d) Auditoría.
   e) Otras.
3. Interpretación de los principios y figuras jurídicas consagradas por la LOPD y desarrolladas por su Reglamento realizada por los tribunales de justicia y por las Agencias de protección de datos.
4. Derechos de los titulares de los datos de carácter personal consagrado por la LOPD y desarrollado por el RLOPD. Forma de hacerlos efectivos en el entorno de una organización:
   a) Acceso.
   b) Rectificación.
   c) Cancelación.
   d) Oposición.

   Impacto de la normativa relativa al impulso sobre la Sociedad de la Información en ha forma en cómo se gestionan estos derechos.
5. Procedimientos administrativos consagrados por la LOPD y desarrollados por el RLOPD. Principios de derecho administrativo que rigen estos procedimientos y normativa administrativa general aplicable.

3. DOMINIO 3: MARCO SECTORIAL DE LA PROTECCIÓN DE DATOS EN ESPAÑA

3.1 ADMINISTRACIÓN ELECTRÓNICA

3.1.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga la capacidad de analizar y detectar las obligaciones en relación a la protección de protección de datos, en el marco de la aplicación de la normativa relativa a la Administración Electrónica, y saber considerar las exigencias de cumplimiento derivadas del cambio en el sistema de tratamiento de datos personales en el ámbito de la Administración Pública, el procedimiento administrativo y la relación entre la Administración y el ciudadano.

3.1.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para identificar los datos personales, protegibles por la Ley, en los procesos internos de la Administración Pública.
2. Disponer de la capacidad para identificar qué tipología de datos podrán ser accesibles a través de la red mediante diarios oficiales o tablones de anuncios electrónicos, preservando el derecho a la protección de datos personales.
3. Disponer de la capacidad para considerar las obligaciones en materia de Administración Electrónica cuyo cumplimiento se debe alinear con las obligaciones en materia de protección de datos.
4. Disponer de la capacidad para identificar los riesgos de seguridad de los datos tratados telemáticamente en sectores jurídico-públicos.
5. Conocer cuáles deben ser los principios básicos de aplicación a la adecuación de la Administración Pública a la Administración Electrónica.
6. Identificar los derechos de los ciudadanos ante el uso de medios telemáticos por la Administración Pública.
7. Disponer del criterio suficiente para identificar los retos a los que el empleado público va a tener que enfrentarse en la modernización de la Administración Pública.

3.1.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Funcionamiento general de la Administración Pública.
2. Obligaciones impuestas por la normativa en materia de Administración Electrónica.
3. Aplicación de los principios de la LOPD en el entorno de la Administración Electrónica.
4. Implantación de las medidas de seguridad necesarias para el cumplimento de la normativa de protección de datos en el ámbito de la Administración Electrónica.

3.2 SALUD

3.2.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato obtenga conocimientos suficientes de las obligaciones que en materia de protección de datos, tiene una organización del sector sanitario de carácter público o privado, que trate datos sensibles. En particular, se pretende que que el candidato sea capaz de determinar las principales obligaciones de contenido jurídico, así como de los requisitos de seguridad (desde un punto de vista organizativo y técnico) para proteger los datos en el sector Salud.

Para ello, se pretende evaluar el conocimiento en aspectos como la definición, implantación y evaluación de los requisitos derivados de la normativa protección de datos personales, y de su adaptación a la normativa específica del sector Salud que afecte a los sistemas de información.

3.2.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad para identificar y definir los ficheros que tratan datos sanitarios, publicarlos e inscribirlos en la Agencia de protección de datos correspondiente.
2. Disponer de la capacidad para definir los requisitos de protección de datos personales específicos para los sistemas de información en el ámbito sanitario.

3. Asegurar la capacidad para definir los procedimientos que garantizan los derechos reconocidos en la normativa sanitaria y en la de protección de datos personales. Concretamente, derecho de acceso, rectificación, cancelación y oposición a un determinado tratamiento de dato sanitario.
4. Aportar soluciones para la implantación de las medidas de seguridad exigidas por la normativa de protección de datos personales, así como asegurar la capacidad suficiente para verificar si las diferentes soluciones implantadas se adaptan además, a las exigencias de la normativa sanitaria y de seguridad.

3.2.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Estructura y funcionamiento de la organización de los Sistemas de Salud.
2. Procedimientos de declaración de los ficheros que tratan datos de carácter personal sanitarios.
3. Normativa relativa al tratamiento de las Historias Clínicas.
4. Normativa específica con relación al derecho de acceso a los datos de salud.
5. Procedimientos que garantizan los derechos de rectificación cancelación y oposición a los datos de la Historia Clínica.

3.3 UNIVERSIDADES PÚBLICAS

3.3.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato obtenga la capacidad suficiente para identificar en el marco de la actividad de las Universidades Públicas aquellas actuaciones afectadas por la normativa de protección de datos.

El candidato deberá poder identificar las obligaciones en el tratamiento de datos de carácter personal, atendiendo al ámbito de la educación y, desde luego al entorno de una universidad pública, así como establecer criterios específicos para proteger los derechos de los interesados, sean estos alumnos, personal docente (PDI) o de administración y servicios (PASS).

Asimismo, deberá disponer de conocimientos suficientes en relación con la aplicación efectiva de las medidas de seguridad necesarias, que garanticen la disponibilidad, confidencialidad e integridad de los datos de carácter personal.

3.3.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para aportar a una universidad pública la estrategia adecuada en cuanto privacidad y protección de datos personales, atendiendo a la diversidad de tratamientos realizados por la Universidad (Consejo Social, asociaciones de alumnos, enseñanza superior y de postgrado, personal interno, relaciones con alumnos extranjeros, régimen de prácticas, investigación, etc.).
2. Asegurar la capacidad para el cumplimiento de las obligaciones registrales aplicables a las Universidades y entes que dependen de las mismas.
3. Disponer de la capacidad suficiente para identificar los supuestos de cesiones de datos entre Universidades y garantizar el cumplimiento de las obligaciones exigidas por al normativa en estos supuestos.
4. Obtener la capacidad para establecer las relaciones contractuales de encargado del tratamiento necesarias con aquellos terceros, dependientes o no de las Universidades que traten datos cuenta de la misma, así como para realizar una correcta articulación jurídica de las mismas.
5. Dotar a cada organización de los procesos internos de respuesta ante el ejercicio de los derechos de acceso, rectificación, cancelación y oposición reconocidos por la LOPD.

3.3.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Estructura y funcionamiento de la universidad pública.
2. Procedimientos de declaración de los ficheros que tratan datos de carácter personal en el ámbito universitario.
3. Normativa relativa al tratamiento de datos de carácter personal en el ámbito universitario.
4. Procedimientos que garantizan los derechos de acceso rectificación cancelación y oposición a los datos en el ámbito de la universidad pública.

3.4 SEGURIDAD PRIVADA Y VIDEOVIGILANCIA

3.4.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga conocimientos suficientes en materia de protección de datos personales de los aspectos específicos que atañen a la instalación y utilización de dispositivos de captación de sonidos y/o imagen en los ámbitos públicos, privados y semipúblicos.

El candidato deberá alcanzar una visión concreta y determinada, considerando de manera específica la incidencia de la normativa de protección de datos y su interrelación con la de seguridad privada.

3.4.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener un conocimiento de las obligaciones derivadas de la normativa de protección de datos en relación con el tratamiento de imágenes con fines de videovigilancia.
2. Obtener un conocimiento de las obligaciones derivadas de la normativa de seguridad privada en relación con el tratamiento de imágenes con fines de videovigilancia.
3. Disponer de la capacidad suficiente para establecer el proceso de puesta a disposición de las imágenes a las autoridades competentes por las empresas de seguridad.
4. Definir obligaciones para empresas de seguridad dedicadas a la instalación, mantenimiento y/o gestión de los servicios de videovigilancia en función del tipo de tratamiento de imágenes.
5. Determinar los aspectos específicos que, según el tipo de tratamiento, rigen para cada uno de los derechos de los titulares de datos personales.

3.4.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Tipos y funcionamiento de las instalaciones de videovigilancia.
2. Obligaciones específicas que aplican en función de los tipos de instalaciones de videovigilancia y los tratamientos que de estas se derivan.
3. Figuras que pueden darse, en virtud del tipo de prestación de servicios de la empresa de seguridad privada (encargado de tratamiento, responsable del fichero y prestador de servicios sin acceso a datos).
4. Supuestos de legitimación para el uso de instalaciones de videovigilancia en entornos públicos y privados.
5. Finalidades diferentes de la seguridad privada en distintos ámbitos: seguridad pública, seguridad ciudadana, control del tráfico y seguridad vial y en los espectáculos deportivos.
6. Diferencias entre un fichero de videovigilancia de las Fuerzas y Cuerpos y Fuerzas de Seguridad del Estado y cualquier fichero de un ente privado
7. Procedimientos que garantizan los derechos de las personas en los tratamientos de imágenes.

3.5 SEGUROS

3.5.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga conocimientos suficientes en materia de protección de datos personales de los aspectos específicos de un Sector económico de gran relevancia. En este sentido, la normativa específica del Sector Seguros ha incorporado cierta regulación específica en materia de protección de datos personales, dentro de la regulación sectorial, además de que existen numerosos pronunciamientos relevantes de la Agencia Española de Protección de Datos que afectan a tal sector. El objetivo fundamental es, por tanto, que el candidato demuestre su conocimiento y su capacidad para aplicar la normativa y pronunciamientos que en materia de protección de datos se han emitido con relación al Sector Seguros.

3.5.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son la identificación de necesidades de cumplimiento normativo en materia de protección de

datos personales en compañías del Sector Seguros (agentes, corredores, aseguradoras, reaseguradoras, etc.), tanto en aspectos generales como en aspectos específicos derivados del Sector Seguros. Y ello tanto con relación a aspectos técnicos, jurídicos y organizativos. Y en particular:

1. Obtener la capacidad suficiente para aportar a una compañía del sector asegurador la estrategia adecuada en cuanto a privacidad y protección de datos personales.
2. Disponer de la capacidad para considerar las implicaciones de la normativa y criterios específicos sobre protección de datos en los diferentes eslabones de la cadena de valor del aseguramiento.
3. Asegurar la capacidad para resolver las cuestiones específicas que puedan afectar a los diferentes tipos de seguros (Autos, Responsabilidad Civil, Vida, Salud, etc.).
4. Dotar a cada organización del sector seguros, en función de su naturaleza y actividad, de los elementos necesarios para la toma de decisión en cuanto a la asimilación de los criterios de interpretación de la normativa general y sectorial emanados de los pronunciamientos de la Agencia Española de Protección de Datos.
5. Aportar las soluciones para difundir dentro de una organización del sector seguros las implicaciones, consecuencias y medidas de adecuación a la normativa sobre datos personales, así como lograr la formación y concienciación de la organización y sus empleados.

3.5.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Funcionamiento general del sector asegurador.
2. Conocimiento de la normativa sectorial reguladora de los seguros.
3. Aplicación de los principios de la LOPD y de las figuras jurídicas consagradas por dicha norma, en el marco de los distintos tratamientos y relaciones que pudieran darse en la cadena de valor del aseguramiento.

4. DOMINIO 4: MARCO INTERNACIONAL Y DE LA UNIÓN EUROPEA

4.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato adquiera los conocimientos necesarios, para garantizar que en el marco de las transferencias internacionales e intraeuropeas de datos realizadas por una organización, se cumpla con las exigencias legales establecidas por la normativa española y europea de Protección de datos personales. Para ello, es necesario que se conozca con profundidad las diferentes organizaciones e instrumentos internacionales y europeos que definen el marco de la realización de estas transferencias.

4.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para aportar una organización la estrategia adecuada de cumplimiento de la normativa española de Protección de datos personales en materia de transferencias internacionales de datos. Para ello, deberá tener un correcto conocimiento de los siguientes conceptos:
    - País con nivel adecuado de protección
    - Consentimiento informado
    - Puerto Seguro
    - Binding Corporate Rules
    - Encargo del tratamiento internacional
2. Disponer de la capacidad suficiente para tipificar la transferencia de datos a terceros Estados y articularlas con las cláusulas contractuales adecuadas.
3. Obtener la capacidad suficiente para lograr el cumplimiento de la LOPD en transferencias a Estados que no proporcionen un nivel adecuado de protección.

4.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Principales instrumentos internacionales y europeos en materia de protección de datos.
2. Concepto y tipologías de transferencias internacionales de datos

1. Conceptos. Transferencia internacional de datos. Conceptos de exportador e importador de datos.
2. Normativa española sobre transferencia internacional de datos.
    1. Principios en materia de transferencia internacional de datos
    2. Principio general en la transferencia internacional de datos: necesidad de protección adecuada en el país tercero.
    3. Principios de contenido y procedimiento.
    4. Principios aplicables a tratamientos específicos.
3. Clases de transferencias en función del estado de destino.
4. Transferencias liberalizadas entre Estados miembros de la UE. Libre flujo de datos entre los países miembros de la Unión Europea.
5. Transferencias a Estados que proporcionen un nivel adecuado de protección.
    1. Adecuación acordada por la Agencia Española de Protección de Datos.
    2. Adecuación acordada por la Comisión de las Comunidades Europeas.
    3. Referencia a la Decisión que instrumenta el Safe Harbour.
6. Transferencias a Estados que no proporcionen un nivel adecuado de protección.
    1. Autorización del Director de la Agencia Española de Protección de Datos. a) Establecimiento de garantías adecuadas. b) Cláusulas contractuales.
    2. Cláusulas contractuales modelo aprobadas por la Comisión Europea. a) La Decisión 2001/497/CE, b) La Decisión 2002/16/CE) La Decisión 2004/915/CE.
    3. Suspensión de las transferencias internacionales.

5. DOMINIO 5: PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN

5.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato tenga conocimientos suficientes en relación con las técnicas necesarias para evitar la revelación no intencionada de datos personales y garantizar que solo son accedidos por las personas que deben hacerlo en virtud de la función o tarea que tiene encomendada.

Así mismo, éste dominio busca medir los conocimientos en seguridad de la información y las principales guías metodológicas que puede aplicar el Data Privacy Officer (DPO) en su trabajo.

Así mismo se evaluaran las medidas específicas de los sistemas de tratamiento no automatizados.

5.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para análisis de los procesos de negocio en los cuales se tratan los activos de información, y en especial los datos de carácter personal.
2. Disponer de la capacidad suficiente para evaluar y valorar el impacto de la normativa de protección de datos en los procesos de negocio.
3. Asegurar la capacidad suficiente para analizar los sistemas de información que sustentan los procesos de negocio.
4. Contar con los criterios adecuados para evaluar y valorar el impacto de la normativa de protección de datos en los sistemas de información.
5. Obtener la capacidad necesaria para verificación de los controles implantados, así como de proponer nuevos controles para aumentar la eficiencia ó efectividad de los existentes ó para regular nuevas necesidades.
6. Trabajar con las áreas para la evaluación de la efectividad y eficiencia de los controles.

5.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Conocimientos de informática generales.
2. Comprensión de los fundamentos de la gestión de riesgos.
3. Conocimientos generales de seguridad de la información.

6. DOMINIO 6: GESTIÓN Y RESPUESTA ANTE INCIDENTES

6.1 OBJETIVO:

El objetivo fundamental de este dominio es que el candidato conozca las técnicas para definir e implantar planes de gestión y respuesta ante incidentes y planes de continuidad de negocio y recuperación de desastres para minimizar el impacto que pueden producir en la organización y recuperar el nivel normal de funcionamiento en el mínimo tiempo posible y con el menor coste posible.

6.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para asegurar que en la organización existen las políticas necesarias para desarrollar el Plan de Gestión de Incidentes y el Plan de Continuidad de Negocio, de acuerdo con ellas.
2. Disponer de la capacidad suficiente para desarrollar una metodología que permita realizar un análisis de los procesos de la organización.
3. Contar con la capacidad suficiente para realizar un análisis de impacto en el negocio (BIA), un análisis de impacto en la privacidad (PIA) y un análisis de riesgos dentro de la organización.
4. Contar con la capacidad suficiente para desarrollar el plan de gestión y respuesta a incidentes que incluya la definición, los objetivos del plan, las políticas, la clasificación, los sistemas de detección, el equipo de respuesta y los niveles correspondientes la notificación y registro, el análisis y evaluación, el escalado y el tipo de soporte, la resolución y restauración de los sistemas afectados, el cierre y la documentación final.
5. Contar con la capacidad suficiente para desarrollar el plan de continuidad del negocio y de recuperación de desastres que incluya la definición, los objetivos del plan, las políticas, las estrategias, la implantación, las pruebas, el mantenimiento y los controles.
6. Contar con la capacidad suficiente para integrar el plan de gestión y respuesta a incidentes con el plan de continuidad del negocio y de recuperación de desastres.
7. Probar y actualizar los planes existentes de forma periódica, así como garantizar que se evalúan periódicamente los riesgos.

6.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Políticas de seguridad de la información relacionadas con la gestión de incidencias y la continuidad del negocio.
2. Diferentes tipos de análisis de la organización:
    1. Análisis de los procesos de negocio.
    2. Análisis de riesgos de seguridad de la información.
    3. Análisis de impacto en el negocio (BIA).
    4. Análisis de impacto en la privacidad (PIA).
3. Procesos y recursos que integran los planes de gestión y respuesta ante incidentes, continuidad de negocio y recuperación de desastres:
    a) Eventos desencadenantes.
    b) Métodos de detección e identificación.
    c) Tratamiento de la información.
    d) Procesos de notificación, registro, comunicación y escalación.
    e) Métodos de contención.
    f) Funciones del personal.
    g) Utilidades y herramientas de detección y resolución.
    h) Practicas de análisis e identificación de las causas.
    i) Procesos para acciones correctivas.
    j) Procesos de copias de seguridad y recuperación de información.
    k) Disponibilidad de sitios alternativos ante desastres.
    l) Objetivo de punto de recuperación (RPO) y objetivo de tiempo de recuperación (RTO).
    m) Establecimiento de prioridades en el proceso de recuperación.
    n) Prácticas posteriores a la recuperación final.
    o) Cuantificación del impacto causado por el daño.

7. DOMINIO 7: CONTROL Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

7.1 OBJETIVO:

El objetivo fundamental de éste dominio es que el candidato tenga conocimientos suficientes para diseñar y aplicar aquellas políticas y procedimientos necesarios para asegurar de forma razonable, que se alcanzan los objetivos de calidad, seguridad, confiabilidad y cumplimiento normativo de la organización.

En éste sentido se debe tener en cuenta que son las auditorías, tanto de los sistemas de información en general, como de protección de datos, las herramientas más adecuadas para los fines mencionados.

7.2 COMPETENCIAS:

Las principales competencias a desarrollar por el candidato en este dominio son:

1. Obtener la capacidad suficiente para definir los objetivos de control de la organización.
2. Disponer de la capacidad suficiente para establecer los procedimientos de control en línea con los objetivos de control definidos.
3. Contar con la capacidad suficiente para establecer las políticas y la estructura de control dentro de la organización
4. Diseñar el plan, el reglamento, los manuales de procedimiento y programas de control que contengan metas, objetivos e indicadores de rendimiento.
5. Establecer mecanismos de control interno en los procesos de sistemas de información.
6. Establecer y realizar auditorías de SI y protección de datos de acuerdo con las normas, guías y mejores prácticas de auditoría para alcanzar los objetivos planificados, comunicando los problemas que surjan, los riesgos potenciales y los resultados a las principales partes interesadas.
7. Validar la eficacia y eficiencia de los procedimientos de control.
8. Definir las excepciones y limitaciones al control.
9. Establecer mecanismos para asegurar la integridad, los valores éticos y la competencia profesional y el compromiso de todos los componentes de la organización.

10. Obtener la capacidad suficiente para asesorar sobre la implementación de prácticas de gerencia y control de riesgos dentro de la organización y, al mismo tiempo, mantener la independencia.
11. Obtener la capacidad para formar y concienciar tanto a la Dirección como al personal, de la importancia de la seguridad de la información y del cumplimiento de la normativa correspondiente.

7.3 CONOCIMIENTOS NECESARIOS:

Los conocimientos que el candidato debe tener en el ámbito de aplicación de este dominio son:

1. Objetivos de control y controles relacionados con Sistemas de Información (CobiT, ISO 27002).
2. Tipos de controles (Controles preventivos, detectivos y correctivos).
3. Controles sobre el personal y sobre los proveedores.
4. Métricas de Calidad (indicadores de objetivos e indicadores de rendimiento).
5. Limitaciones al Control Interno.
6. Normas, guías y procedimientos de auditoría de Sistemas de Información de ISACA y del Código de Ética Profesional.
7. Prácticas y técnicas de auditoría de SI y técnicas para recolectar información y preservar evidencia (observación, indagación, entrevista, herramientas y técnicas de auditoría computarizada (CAATT) y medios electrónicos).
8. Métodos y herramientas de evaluación de riesgos en el contexto de una auditoría.
9. Técnicas de reporte y comunicación (facilitación, negociación y resolución de conflictos).
10. Autoevaluación de control (CSA) y técnicas de auditoría continua.

8. NORMATIVA DE REFERENCIA

8.1 TODOS LOS DOMINIOS

1. Constitución Española de 1978.
2. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
3. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
4. Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

8.2 DOMINIO 1: FUNDAMENTOS

1. Convenio Europeo por la protección de los Derechos humanos y libertades fundamentales de 4 de noviembre de 1950.
2. Convenio 108 del Consejo de Europa, de 28 de enero de 1981.
3. Protocolo adicional del Convenio nº 108, de 8 de noviembre de 2001.
4. Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
5. Directiva 97/66/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las Telecomunicaciones.
6. Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (Directiva que deroga la anterior).
7. Directiva 2006/24/CE, sobre conservación de datos guardados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
8. Reglamento 45/2001/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios a la libre circulación de estos datos.

8.3 DOMINIO 3: MARCO SECTORIAL

8.3.1 ADMINISTRACIÓN ELECTRÓNICA

1. Decisión 1720/1999/CE del parlamento europeo y del consejo de 12 de julio de 1999 por la que se aprueba un conjunto de acciones y medidas al objeto de garantizar la interoperabilidad de las redes telemáticas transeuropeas destinadas al intercambio electrónico de datos entre administraciones (IDA), así como el acceso a las mismas.
2. Ley 30/1992, de 26 de noviembre, Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
3. Ley 10/2001, de 13 de julio, de archivos y documentos.
4. Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los servicios públicos.
5. Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la Información.
6. Real Decreto 263/1996, de 16 febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.
7. Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
8. **Ley 2/2011, de 4 de marzo, de Economía Sostenible.**
9. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición dl documento nacional de identidad y sus certificados de firma electrónica.
10. Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
11. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
12. **Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.**

8.3.2 SALUD

1. Convenio del Consejo de Europa sobre el respeto a los derechos humanos y la biomedicina 1997
2. Ley 14/1986, de 25 de abril, General de Sanidad.
3. Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida.
4. Ley 25/1990, de 20 de diciembre, del Medicamento.

5. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
6. Ley 16/2003, de 28 de marzo, de cohesión y calidad del Sistema Nacional de Salud.
7. Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesionales Sanitarias.
8. Ley 45/2003, de 21 de noviembre, por la que se modifica la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida.

8.3.3 UNIVERSIDADES

1. Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

8.3.4 VIDEOVIGILANCIA Y SEGURIDAD PRIVADA

1. Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Dereco al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.
2. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
3. Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana.
4. Ley 23/1992, de 30 de julio, de Seguridad Privada.
5. Real Decreto 2364/1994, de 9 de diciembre, que aprueba el Reglamento de Seguridad Privada.
6. Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
7. Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.

8.3.5 SEGUROS

1. Ley 50/1980, de 8 de octubre, de Contrato de Seguro.
2. Ley 20/2005, de 14 de noviembre, sobre la creación del Registro de Contratos de Seguros de cobertura de fallecimiento.
3. Ley 26/2006, de 17 de julio, de mediación de seguros y reaseguros privados.
4. Texto Refundido de la Ley de Ordenación y Supervisión de los Seguros Privados aprobado por Real Decreto Legislativo 6/2004, de 29 de octubre.

5. Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores.

8.4 DOMINIO 4: MARCO INTERNACIONAL Y DE LA UNIÓN EUROPEA

1. Convenio 108 del Consejo de Europa, de 28 de enero de 1981.
2. Protocolo adicional del Convenio nº 108, de 8 de noviembre de 2001.
3. Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
4. Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 y Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.
5. Acuerdos de Puerto Seguro, Comisión Europea, Decisión de 26 de Julio de 2000

9. BIBLIOGRAFÍA, DOCUMENTACIÓN Y SITIOS WEB DE REFERENCIA

9.1 TODOS LOS DOMINIOS

1. APARICIO SALOMÓN, Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal, Aranzadi, Pamplona, 2000.
2. BRANDEIS y WARREN, "The Right to Privacy", en Harvard Law Review, vol. IV, núm. 5, 1890, passim. Trad., "El derecho a la intimidad", Editorial Civitas, Madrid, 1995.
3. HONDIUS F., "A decade internacional Data Protección", NILR, vol. 30, núm. 2, 1983.
4. FACTBOOK PROTECCIÓN DE DATOS PERSONALES, Écija Abogados, Aranzadi 2008.
5. ORTEGA GIMÉNEZ, Alfonso, Guía práctica de protección de datos personales para abogados, Difusión Jurídica y Temas de Actualidad, Madrid 2008.
6. REBOLLO DELGADO, Lucrecio y SERRANO PEREZ María Mercedes, Introducción a la Protección de Datos, Ed. Dykinson, Madrid, 2006.
7. VALERO TORRIJOS, Julián y FERNANDEZ SALMERÓN, Manuel, "Procedimientos administrativos tramitados por la Agencia Española de Protección de Datos", Protección de Datos: Comentarios a la LOPD y su Reglamento de Desarrollo, Tirant lo blanch, Valencia, 2009.
8. GARCÍA AMEZ Javier.«Una mirada a la protección de datos de carácter personal». Actualidad Administrativa, núm. 18, quincena del 16 al 31 Oct. 2006, pág. 2188, tomo 2.
9. Agencia Española de Protección de Datos: http://www.agpd.es
10. Agencia de Protección de Datos de la Comunidad de Madrid: http://madrid.org
11. Agencia Catalana de Protección de Datos: http://www.apd.cat

9.2 DOMINIO 2: MARCO SECTORIAL

9.2.1 ADMINISTRACIÓN ELECTRÓNICA

1. CERRILLO, A "e-Administración" Ed. UOC (2008).
2. CERRILLO, A "La protección de datos en la administración electrónica." Ed. Aranzadi (2009).
3. GALINDO, F "Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento" Ed. Prensas Universitarias de Zaragoza (2010).
4. GAMERO Casado, E. y Valero Torrijos, J. "La Ley de Administración Electrónica. Comentario sistemático L.1/2007, 22 junio, acceso electrónico ciudadanos servicios. " Ed. Aranzadi (2008).
5. PARADA. R. "Derecho Administrativo II. Organización y Empleo Público" Ed. Marcial Pons (1998).
6. Desarrollo de la Administración Electrónica en la Unión Europea http://www.epractice.eu

1. Guía práctica de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP) Comisión de Modernización y Calidad de la FEMP http://www.csi.map.es/csi/pdf/guia-femp.pdf
2. La Administración Electrónica y el Servicios a los Ciudadanos http://www.meh.es/Documentacion/Publico/SGT/e-administracion.pdf
3. Plan de Acción i2010: http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm
4. Plan de acción sobre administración electrónica i2010: Acelerar la administración electrónica en Europa en beneficio de todos (COM(2006) 173 final) http://www.csi.map.es/csi/pdf/com_2006_0173_f_es_acte.pdf
5. Informe Jurídico 0052/2009 de la Agencia Española de Protección de Datos sobre la Utilización de datos cedidos por otras Administraciones. Informe Jurídico 0217/2009 de la Agencia Española de Protección de Datos sobre Documentos electrónicos alojados en una plataforma de depósito de documentos de la administración pública
6. Recomendación 2/2008, de 25 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre publicación de datos personales en boletines y diarios oficiales en Internet, en sitios webs institucionales y en otros medios electrónicos y telemáticos
7. Recomendación 3/2008, de 30 de abril, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre tratamiento de datos de carácter personal en servicios de administración electrónica.
8. Consejo superior de Administración Electrónica: http://www.csi.map.es/

9.2.2 SALUD

1. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME) - Grupo de trabajo sobre protección de datos del artículo 29
2. Recomendación 2/2004, de la Agencia de Datos de la Comunidad de Madrid sobre la custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas.

9.2.3 UNIVERSIDADES

1. Bello Paredes, Santiago A; Caro Muñoz, Ana I (Dirs). "La administración electrónica y la protección de datos encuentro nacional sobre transparencia en la gestión universitaria" Ed. Universidad de Burgos (2009).
2. González García. Julio. V (Dir). "Comentarios a la Ley Orgánica de Universidades." Ed. Civitas (2009).
3. Peña Callejas, P "Universidades Públicas. Régimen Jurídico. Informe sobre casos prácticos.". Ed. Instituto Nacional de Administración Pública (2008).
4. Informe Jurídico nº 0662/2008 de la Agencia Española de Protección de Datos.
5. Informe Jurídico 0379/2009 de la Agencia Española de Protección de Datos.
6. Informe Jurídico 0376/2008 de la Agencia Española de Protección de Datos.
7. Resolución de archivo de actuaciones de la Agencia Española de Protección de Datos Expediente Nº: E/01048/2007.
8. Resolución de la Agencia Española de Protección de Datos Procedimiento Nº AP/00070/2008.
9. Agencia de Protección de Datos de la Comunidad de Madrid. "Guía de Protección de Datos para Universidades" Ed. Civitas (2004).

9.2.4 VIDEOVIGILANCIA Y SEGURIDAD PRIVADA

1. Guía de Videovigilancia de la Agencia Española de Protección de Datos.
2. Dictamen 4/2004, de fecha 11/02/2004, del Grupo del artículo 29 relativo al tratamiento de datos personales mediante vigilancia por videocámara.
3. Informes jurídicos sobre videovigilancia de la AEPD:
4. Recomendaciones de la AEPD: Plan sectorial de oficio sobre Videocámaras en Internet (Junio 2009):

1. Informe 0650/2009 de la AEPD, sobre la Modificación de los sistemas de video vigilancia por la Ley Ómnibus.
2. Informe 0569/2009 del Gabinete Jurídico de la AEPD, sobre empresas de seguridad privadas contratadas por Ayuntamientos.

9.2.5 SEGUROS

1. Recomendaciones de la Agencia de Protección de Datos en relación con el Fichero Histórico de Seguros del Automóvil, del que es Responsable la Unión Española de Entidades Aseguradoras y Reaseguradoras, para su adecuación a la legislación vigente en materia de protección de datos.
2. Recomendaciones de la Agencia de Protección de Datos en relación con el Fichero Histórico de Seguros del Automóvil, del que es Responsable la Unión Española de Entidades Aseguradoras y Reaseguradoras, para su adecuación a la legislación vigente en materia de protección de datos.
3. Resolución R/00397/2003 (PS/00027/2003), de la Agencia Española de Protección de Datos.
4. Informe 0463/2009 de la Agencia Española de Protección de Datos
5. Informe 0363/2008 de la Agencia Española de Protección de Datos
6. Informe 0449/2004 de la Agencia Española de Protección de Datos
7. Informe 0526/2003 de la Agencia Española de Protección de Datos
8. Informe 0359/2002 de la Agencia Española de Protección de Datos
9. La Asociación Empresarial del Seguro (UNESPA) http://www.unespa.es
10. Tecnologías de la Información y Comunicación para el Sector Asegurador en España. http://www.tirea.com.
11. Consorcio de Compensación de Seguros http://www.consorseguros.es/web/guest/31
12. Dirección General de Seguros y Fondos de Pensiones http://www.dgsfp.meh.es

9.3 DOMINIO 3: MARCO INTERNACIONAL Y DE LA UNIÓN EUROPEA

1. ACED FÉLEZ, D. EMILIO, "Transferencia internacional de datos", PROTECCIÓN DE DATOS DE CARACTER PERSONAL EN IBEROAMÉRICA (II Encuentro Iberoamericano de protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003, Tirant lo blanch, Valencia, 2006.
2. BARCELÓ, Rosa y PÉREZ ASINARI, María Verónica, "Transferencia internacional de datos personales", Protección de Datos: Comentarios a la LOPD y su Reglamento de Desarrollo, Tirant lo blanch, Valencia, 2009.
3. ESTADELLA YUSTE, Olga, La protección de la intimidad frente a la transmisión internacional de datos personales, Ed. Tecnos, Madrid, 1995.

4. RIPOLL CARULLA, Santiago, "El movimiento internacional de datos. Legislación española y derecho internacional", Telos, núm.37, marzo- mayo 1994.
5. SANCHO VILLA, Diana, Transferencia internacional de datos personales, Agencia de Protección de Datos (Premio Protección de Datos Personales VI Edición), Madrid, 2003.
7. Auditoria de protección de datos adaptado al nuevo reglamento II edición – Editorial BOSCH.

9.4 GESTIÓN Y RESPUESTA ANTE INCIDENTES

1. ITIL V.3
2. ISO20000
3. Familia ISO 27000
4. NIST SP 800-61
5. BS 25999
6. Manual de preparación del examen CISA
7. Manual de preparación del examen CISM
8. Information Systems Audit and Control Association www.isaca.org
9. It Governance Institute www.itgi.org
10. DRI International www.drii.org
11. Contingency Planning & Management www.contingencyplanning.com

9.5 CONTROL Y AUDITORÍA

1. Familia ISO 27000
2. COBIT 4.0 de IT Governance Institute.
3. COSO.
4. Marco para la práctica profesional de la auditoría interna del Instituto de Auditores Internos.
5. Auditoría de la protección de datos de editorial Practik Bosch.
6. La protección de datos de carácter personal en los centros de trabajo de editorial Cinca.
7. Seguridad de la información de Paraninfo.
8. La LOPD, análisis y comentario de su jurisprudencia de editorial Lex Nova.
4. Guías traducidas y editadas por ISMS Forum Spain:
    1. Medidas y métricas.
    2. Instaurar buenas prácticas globales en Gestión de Continuidad de Negocio.
    3. Implementación y certificación de los sistemas de seguridad de la información.

10. Agradecimientos

Nuestros más sinceros agradecimientos a todas las personas que han colaborado en la creación de esta certificación:

o	Miguel Ángel	Ballesteros Ballesteros	Auditor en CEPSA
o	Antoni	Bosch Pujol	Director Institute of Audit & IT-Governance y Director Data Privacy Institute (DPI)
o	Josep	Cabañete-Pérez	Abogado-CISA en A2SI
o	Francisco Javier	Carbayo Vázquez	Gerente del área de Governance, Risk & Compliance de Ecija, CISM, CDPP
o	Miguel	Cebrián Lindström	Risk and Compliance Manager
o	Francesc	Flores González	Auditor de SI. Consultor de SI, IT Governance y Privacidad
o	Alejandro	Gacitúa	Abogado y Consultor en Derecho y Tecnología
o	Anna	García Martínez	Responsable de Seguridad de Sistemas de Información en Generalitat de Catalunya
o	Ana	Gonzalez Romo	Gestora de Seguridad en Endesa
o	Adolfo	Hernández	Gerente del área de Governance, Risk & Compliance de Ecija, CDPP, CISM, CISA, CISSP, ITILf
o	Ana	Iparraguirre Jimenez	Coordinadora LOPD en FCC VERSIA, S.A.
o	Maria José	Lacunza Gonzalez	Abogada especialista en Derecho de las Tecnologías
o	Joan Lluís	Pérez-Francesch	Liberty and security group at Universitat Autònoma de Barcelona
o	Antonio	Ramos	Socio Director de n+1 Intelligence & Research, CEO de leet security y Presidente de ISACA Madrid Chapter
o	Soledad	Romero Jiménez	Consultora legal en Ingenia
o	Carlos Alberto	Sáiz Peña	Socio Responsable del área de Governance, Risk & Compliance de Ecija