



**INFORME Y ESTUDIO  
DE ADECUACIÓN A LA  
LEY ORGÁNICA DE PROTECCIÓN DE DATOS  
15/1999**

**DATA CONSULTORES Y AUDITORES DE PROTECCIÓN DE DATOS  
S.R.L.**

**C/ Fray Luís de Granada nº 13, 2º-A**

**14008 Córdoba**

**Tlef.: 957479522-692571337**

**Fax: 957488492**

**[consultoria@dataconsultores.com](mailto:consultoria@dataconsultores.com)**

**[www.dataconsultores.com](http://www.dataconsultores.com)**

**CONTENIDO:**

**I.- PRESENTACIÓN\_\_\_\_\_pág.3**

**1. Data Consultores. Empresa y servicios\_\_\_\_\_pág.4**

**II.- FUNDAMENTOS JURÍDICOS\_\_\_\_\_pág. 6**

**2. Glosario de términos**

**3. Resumen de obligaciones, medidas de seguridad y sanciones**

**III.- ESTUDIO\_\_\_\_\_pág.12**

## I.- PRESENTACIÓN

La Ley Orgánica de Protección de Datos tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

La Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Desde DATA Consultores se pretende ofrecer una solución global de servicios al amparo de esta ley, actuando en base a unos procedimientos establecidos en diferentes formatos que facilitan el proceso de implantación en la medida concreta que requiere el cliente, a fin de dar cumplimiento a las obligaciones que la Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre, (en adelante LOPD) impone para aquellas personas físicas o jurídicas que posean ficheros con datos de carácter personal, así como lo establecido en el Reglamento de Seguridad (R.D. 994/99 de 11 de junio) que desarrolla la mencionada Ley Orgánica y que establece la obligación de las empresas de poner en marcha diversas medidas destinadas a garantizar la protección de dichos datos, afectando a sistemas informáticos, archivos de soportes de almacenamiento, personal, procedimientos operativos, etc.

### I.1.- Data Consultores ¿Quiénes somos?

**DATA CONSULTORES** es una compañía integrada por profesionales de reconocido prestigio en el sector informático andaluz, que nace con el objetivo de continuar manteniendo el nivel de satisfacción que exigen sus propios clientes.

**DATA CONSULTORES** está respaldada por un competente equipo jurídico, así como por empresas líderes en el sector de las nuevas tecnologías como son: **ICONOS SOFTWARE, DAFOS TRAINING y ASTIVIA TECNOLOGÍAS AVANZADAS.**

**DATA CONSULTORES**, además de contratos de prestación de servicios con empresas y profesionales, tiene firmados convenios de colaboración, que ponen de manifiesto la seriedad y solvencia de la empresa, con diversas entidades públicas como:

**Confederación de Empresarios de Córdoba (CECO)**

**Cámara Oficial de Comercio e Industria de la Provincia de Córdoba**

**Ilustre Colegio Oficial de Abogados de Córdoba**

**Ilustre Colegio Oficial de Abogados de Lucena**

**Ilustre Colegio Oficial de Procuradores,**

**Ilustre Colegio Oficial de Médicos de Córdoba,**

**Ilustre Colegio Oficial de Veterinarios de Córdoba**

**VIMCOSA**

**CONSORCIO DE TURISMO**

**CONSORCIO ORQUESTA DE CÓRDOBA**

**CECOSAM. Cementerios Municipales de Córdoba**

El hecho de la obligatoriedad que supone para las empresas, entidades y profesionales, el declarar e inscribir en la Agencia de Protección de Datos, aquellos ficheros que contengan datos de carácter personal, propicia la colaboración entre los diferentes profesionales de otras empresas, para iniciar el desarrollo de las plataformas que garanticen el servicio y la tranquilidad de sus clientes, en esta materia

### A) Descripción de Data Consultores:

El personal técnico de Data Consultores está dividido en diferentes áreas de actuación, con objeto de poder centralizar los niveles de responsabilidad de cara a sus clientes. No obstante, el perfil de los consultores técnicos está sometido a continuos procesos de formación en las exigencias que dictamina la ley, así como de los requisitos técnico-informáticos necesarios para realizar una gestión de consultoría adecuada. Estas áreas departamentales son las siguientes:

#### Área Técnica Informática:

Los consultores informáticos de esta área procederán a realizar una localización de los ficheros susceptibles de declaración, así como a realizar labores de asesoramiento técnico sobre una correcta política de usuarios.

#### Área Técnica Jurídica:

Inherente al contrato que el cliente firma con Data Consultores, se incluye el servicio permanente de un gabinete jurídico representado en la sociedad, que asumirá la defensa jurídica ante inspecciones de la Agencia de Protección de Datos, y reclamaciones o denuncias de terceros.

#### Área de Desarrollo:

Con objeto de mantener el aplicativo software completamente actualizado y conforme a las exigencias de la LOPD, DATA CONSULTORES dispone de un gabinete de desarrollo o programación que realizará esta labor, así como la implantación en modo local de estos aplicativos.

#### Área de Internet:

Al igual que sucede con el personal del área de desarrollo y programación, para aquellos clientes que opten por mantener personalmente las incidencias que afecten al documento de seguridad, DATA CONSULTORES dispone de técnicos específicos en materia Web para garantizar la privacidad y niveles de accesibilidad de los usuarios a la Plataforma.

#### Auditorías y Control de Incidencias:

DATA CONSULTORES prestará de forma presencial la Auditoria exigida por el artículo 17 del reglamento contemplado en el RD 994/1999. Asimismo redactará el Informe de Auditoria donde DATA CONSULTORES proporcionará las acciones o medidas correctoras en su caso.

DATA CONSULTORES pone a disposición de sus clientes un servicio hot line en materia de consultoría tanto técnica como jurídica.

DATA CONSULTORES realiza las auditorías periódicas de los sistemas de información del cliente dependiendo del nivel de seguridad que requiera el mismo.

#### Documentación:

Una vez realizado el servicio de Consultoría previa por parte del personal técnico, se pondrán en marcha los mecanismos necesarios para el desarrollo de aquellos formularios o contratos que tengan que vincularse directamente a la protección de los datos del Cliente, (contratos con personal laboral, proveedores de servicios con acceso a datos, etc...). Esta gestión se refiere a la política de privacidad que se necesita disponer en las instalaciones del cliente ante una posible inspección de la APD.

#### Formación:

El cliente podrá acceder de forma gratuita a todos aquellos seminarios o monográficos que organice DATA CONSULTORES, con objeto de mantenerle informado sobre aquellos aspectos que influyan en alguna medida sobre la LOPD. Estos seminarios se organizan en nuestras instalaciones de forma aleatoria, pudiendo el cliente contratar un servicio específico de formación en sus propias instalaciones para su personal y previa solicitud de presupuestos para dicho servicio.

#### Defensa Jurídica:

En caso de inspección de la APD, o ante denuncias de terceros a causa de una supuesta infracción de la LOPD, Data Consultores pondrá a su disposición un gabinete jurídico para el asesoramiento y asistencia ante la APD., en vía administrativa.

## B) Productos y Servicios

Los servicios que **DATA CONSULTORES** presta a empresas, profesionales y colectivos son los que se detallan a continuación:

### 1.- Consultoría y Declaración inicial de los ficheros del cliente ante la APD

Esta consultoría inicial se realiza personando en las instalaciones del cliente un técnico de DATA CONSULTORES, para determinar el número de ficheros existentes y susceptibles de declarar, así como su correcta clasificación de nivel, en función de su contenido y finalidad. Asimismo, redactaremos la documentación necesaria para su inscripción en el Registro General de la Agencia de Protección de Datos, que finalmente formalizaremos.

### 2.- Elaboración del Documento de Seguridad, exigido por el Real Decreto 994/1999, sobre aquellos ficheros que contengan datos de carácter personal en cualquiera de sus niveles de protección.

Se expondrá en este documento las diferentes medidas de seguridad técnicas y administrativas que permitan garantizar la seguridad de los ficheros. Se tendrá en cuenta la política de usuarios con acceso a estos datos, personal laboral, empresas de servicios, equipos informáticos y sistemas, etc...

### 3.-Mantenimiento del Documento de Seguridad.

Una vez el cliente disponga de su Documento de Seguridad, tendrá la obligación de mantenerlo completamente actualizado, registrando todas aquellas incidencias que puedan afectar directamente sobre la política de protección de datos, y adjuntándolas conforme a la disposición legal en el documento original. De ahí precisamente la importancia de su mantenimiento, procurando de forma permanente su revisión y/o actualizando, y garantizando su correcta adaptación ante posibles actuaciones inspectoras de la APD.

**DATA CONSULTORES** proporcionará al cliente diferentes modalidades para que una vez elaborado el Documento de Seguridad de sus datos, y transcurrido el primer año de vigencia del contrato de servicios, éste pueda elegir la modalidad de mantenimiento de las incidencias que se vayan sucediendo y que afecten al contenido de dicho documento. Estas opciones son las siguientes:

- **DATA CONSULTORES** dispone de una plataforma Portal Web, que permite la autenticación de los usuarios registrados, para acceder de forma privada y segura a su propia base documental, y así poder gestionar personalmente sus incidencias y por consiguiente la actualización permanente de su documento.
- En el caso de que el cliente opte por la alternativa en la que **DATA CONSULTORES** asuma toda la gestión relacionada con la seguridad de sus datos, se procederá a la firma de un contrato de servicios, en el que nos subrogamos a dicha responsabilidad realizando las acciones que sean necesarias para garantizar la adaptación del documento, conforme a las exigencias y cambios que dicte la ley.

## II.- FUNDAMENTOS JURÍDICOS

- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
- *Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.*
- *Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.*
- *RESOLUCIÓN de 22 de junio de 2001, de la Subsecretaría, por la que se dispone la publicación del Acuerdo de Consejo de Ministros por el que se concreta el plazo para la implantación de medidas de seguridad de nivel alto en determinados sistemas de información.*
- *REAL DECRETO 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio.*

### II.1.- GLOSARIO DE TÉRMINOS

A los efectos de la Ley Orgánica se entenderá por:

- a. **Datos de carácter personal:** cualquier información concerniente a personas físicas identificadas o identificables.
- b. **Fichero:** todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- c. **Tratamiento de datos:** operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- d. **Responsable del fichero:** persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- e. **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
- f. **Procedimiento de disociación:** todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
- g. **Encargado del tratamiento:** la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- h. **Consentimiento del interesado:** toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.
- i. **Cesión o comunicación de datos:** toda revelación de datos realizada a una persona distinta del interesado.
- j. **Fuentes accesibles al público:** aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

## II.2.- RESUMEN DE OBLIGACIONES, NIVELES DE SEGURIDAD Y SANCIONES

### **1.- OBLIGACIONES LEGALES DE LA NORMATIVA DE PROTECCIÓN DE DATOS**

#### **OBLIGACIONES (EXTRACTO):**

#### **\* Ley Orgánica de Protección de Datos de Carácter Personal 15/1999, de 13 de Diciembre.**

##### **Artículo 1.** Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

##### **Artículo 2.** Ámbito de aplicación.

La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado

(...)

##### **Artículo 25. Creación**

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la, persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

##### **Artículo 26. Notificación e inscripción registral**

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

(...)

#### **\*Real Decreto 994/1999, DE 11 DE JUNIO**

##### **Artículo 1. Ámbito de aplicación y fines.**

El presente Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal sujetos al régimen de la Ley Orgánica 5/1992, de 20 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal.

##### **Artículo 3. Niveles de seguridad.**

1. Las medidas de seguridad exigibles se clasifican en tres niveles: básico, medio y alto.
2. Dichos niveles se establecen atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

##### **Artículo 4. Aplicación de los niveles de seguridad.**

1. Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.
2. Los ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y aquellos ficheros cuyo funcionamiento se rija por el artículo 28 de la Ley Orgánica 5/1992, deberán reunir, además de las medidas de nivel básico, las calificadas como de nivel medio.
3. Los ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los que contengan datos recabados para fines policiales sin consentimiento de las personas afectadas deberán reunir, además de las medidas de nivel básico y medio, las calificadas de nivel alto.

## CAPÍTULO II

### Medidas de seguridad de nivel básico

#### Artículo 8. *Documento de seguridad.*

- El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.
- El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

#### Artículo 9. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas, de acuerdo con lo previsto en el artículo 8.2.c).
2. El responsable del fichero adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento

#### Artículo 10. *Registro de incidencias.*

El procedimiento de notificación y gestión de incidencias contendrá necesariamente un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubieran derivado de la misma.

#### Artículo 11. *Identificación y autenticación.*

1. El responsable del fichero se encargará de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

#### Artículo 12. *Control de acceso.*

1. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.

#### Artículo 13. *Gestión de soportes.*

1. Los soportes informáticos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en el documento de seguridad.

#### Artículo 14. *Copias de respaldo y recuperación.*

1. El responsable de fichero se encargará de verificar la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
2. Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos deberá garantizar su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
3. Deberán realizarse copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

## CAPÍTULO III

### Medidas de seguridad a nivel medio

#### Artículo 15. *Documento de seguridad.*

El documento de seguridad deberá contener, además de lo dispuesto en el artículo 8 del presente Reglamento, la identificación del responsable o responsables de seguridad, los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

#### Artículo 16. *Responsable de seguridad.*

El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.

#### Artículo 17. *Auditoría.*

1. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

#### Artículo 18. *Identificación y autenticación.*

1. El responsable del fichero establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

#### Artículo 19. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información con datos de carácter personal.

#### Artículo 20. *Gestión de soportes.*

1. Deberá establecerse un sistema de registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

#### Artículo 21. *Registro de incidencias.*

## INFORME Y ESTUDIO DE ADECUACIÓN A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

1. En el registro regulado en el artículo 10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

### **Artículo 22. Pruebas con datos reales.**

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

## **CAPÍTULO IV**

### **Medidas de seguridad de nivel alto**

#### **Artículo 23. Distribución de soportes**

La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

#### **Artículo 24. Registro de accesos.**

1. De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

#### **Artículo 25. Copias de respaldo y recuperación.**

Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

#### **Artículo 26. Telecomunicaciones.**

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

**2.- NIVELES DE SEGURIDAD**

La ley identifica tres niveles de medidas de seguridad, **BÁSICO**, **MEDIO** y **ALTO**, los cuales deberán ser adoptados en función de los distintos tipos de datos personales (datos de salud, ideología, religión, creencias, infracciones administrativas, de morosidad, etc).

	<b>NIVEL BÁSICO</b>
<b>TIPO DE DATOS</b>	<ul style="list-style-type: none"> <li>• Nombre</li> <li>• Apellidos</li> <li>• Direcciones de contacto (tanto físicas como electrónicas)</li> <li>• Teléfono (tanto fijo como móvil)</li> <li>• Otros</li> </ul>
<b>MEDIDAS SEGURIDAD OBLIGATORIAS</b>	<ul style="list-style-type: none"> <li>• Documento de seguridad</li> <li>• Régimen de funciones y obligaciones del personal</li> <li>• Registro de incidencias</li> <li>• Identificación y autenticación de usuarios</li> <li>• Control de acceso</li> <li>• Gestión de soportes</li> <li>• Copias de respaldo y recuperación</li> </ul>
	<b>NIVEL MEDIO</b>
<b>TIPO DE DATOS</b>	<ul style="list-style-type: none"> <li>• Comisión infracciones penales y administrativas</li> <li>• Información de Hacienda Pública</li> <li>• Información de servicios financieros</li> <li>• Información sobre evaluación personal (currículum)</li> </ul>
<b>MEDIDAS SEGURIDAD OBLIGATORIAS</b>	<ul style="list-style-type: none"> <li>• Medidas de seguridad de nivel básico</li> <li>• Responsable de Seguridad</li> <li>• Auditoría bianual</li> <li>• Medidas adicionales de Identificación y autenticación de usuarios</li> <li>• Control de acceso físico</li> </ul>
	<b>NIVEL ALTO</b>
<b>TIPO DE DATOS</b>	<ul style="list-style-type: none"> <li>• Ideología</li> <li>• Religión</li> <li>• Creencias</li> <li>• Origen racial</li> <li>• Salud</li> <li>• Vida sexual</li> </ul>
<b>MEDIDAS SEGURIDAD OBLIGATORIAS</b>	<ul style="list-style-type: none"> <li>• Medidas de seguridad de nivel básico y medio</li> <li>• Seguridad en la distribución de soportes</li> <li>• Registro de accesos</li> <li>• Medidas adicionales de copias de respaldo</li> <li>• Cifrado de telecomunicaciones</li> </ul>

## 3.- SANCIONES

Se establecen una serie de sanciones a los responsables de los ficheros y a los encargados del tratamiento de los ficheros que contengan datos de carácter personal. Estas se clasifican en leves, graves y muy graves, atendiendo a la infracción cometida.

	SANCIONES
LEVES	Multa de 601,01 € a 60.101,21 € (100.000 a 10.000.000 de pesetas)
GRAVES	Multa de 60.101,21 € a 300.506,05 € (10.000.000 a 50.000.000 pesetas)
MUY GRAVES	Multa de 300.506,05 € a 601.012,10 € (50.000.000 a 100.000.000 de pesetas)

Es de vital importancia que las empresas y profesionales, que recojan datos de carácter personal se adecuen a la normativa de protección de datos.

## III.- ESTUDIO

### A.- MEDIDAS A DESARROLLAR

#### 1.- AUDITORIA PREVIA

- ⇒ **Análisis y detección de las estructuras de bases de datos.**
- ⇒ **Valoración de Niveles de Seguridad**
- ⇒ **Detección de usuarios y accesos**
- ⇒ **Estudio de la política de seguridad y medidas desarrolladas.**
- ⇒ **Informe de adecuación y deficiencias**

#### 2.- CONSULTORÍA

- 1. Elaboración de la documentación necesaria para la inscripción de los ficheros.**
- 2. Elaboración del Documento de Seguridad, de acuerdo al nivel de seguridad exigido.**
- 3. Actualización de la declaración de ficheros, incidencias y medidas de seguridad.**
- 4. Realización de documentación para control de usuarios, obligación de información y derechos de acceso.**
- 5. Elaboración de contratos y documentación necesaria para la adecuación a la LOPD**

#### 3.-MANTENIMIENTO

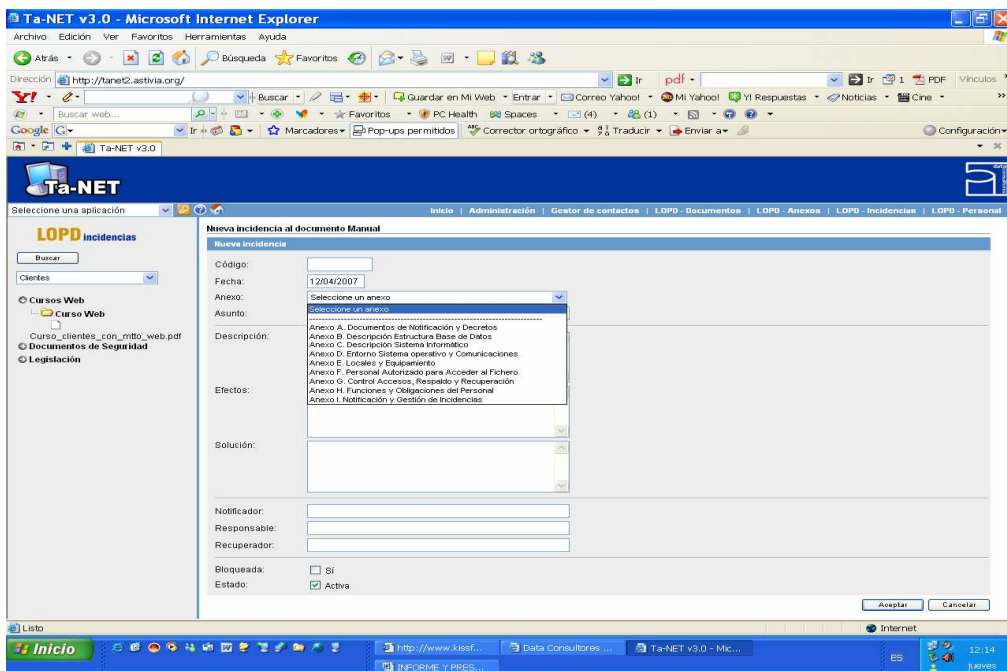
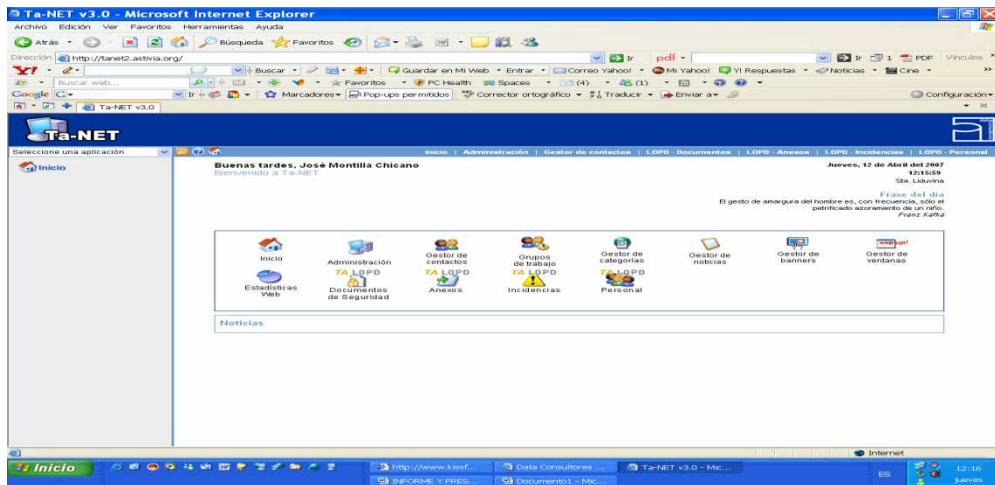
- 1. Actualización y seguimiento de las obligaciones normativas establecidas por la LOPD, a través de operativo on-line.**
- 2. Auditorias preceptivas**
- 3. Asesoramiento y representación jurídica.**
- 4. Formación en relación a la implantación y mantenimiento de las medidas de seguridad establecidas en la Ley de Protección de Datos y LSSI.**

El servicio de mantenimiento se ofrece en:

- **Modo Integral:** Data Consultores gestionará todo lo necesario para mantener el Documento de Seguridad actualizado; el cliente solo deberá comunicarnos las incidencias producidas.
- **Pack DataWeb** que al igual que la anterior permite que el Documento de Seguridad este siempre actualizado por el propio cliente. Se suministra con las claves necesarias para una conexión a Internet, una Cuenta de Correo Electrónico y un acceso privado a su área Intranet.

## INFORME Y ESTUDIO DE ADECUACIÓN A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Desarrollándose a través de un operativo tecnológico, basado en las directrices de la Agencia Española de Protección de Datos que agiliza y maximiza los resultados de gestión de control de la información:



**DATA CONSULTORES** tiene firmados convenios de colaboración, a través de los cuales se ofrecen tarifas reducidas preferentes, con diversas entidades como la Confederación de Empresarios de Córdoba (CECO), el Ilustre Colegio de Abogados de Córdoba, el Ilustre Colegio de Procuradores, el Ilustre Colegio de Médicos de Córdoba.



**Desde Data Consultores nos ponemos a su disposición para asesorarle sin ningún compromiso. Contacte con nosotros.**

DATA CONSULTORES Y AUDITORES DE PROTECCIÓN DE DATOS S.R.L.  
C/ Fray Luís de Granada nº 13, 2º-A  
14008 Córdoba  
Tlef.: 957479522-692571337  
Fax: 957488492  
[consultoria@dataconsultores.com](mailto:consultoria@dataconsultores.com) [www.dataconsultores.com](http://www.dataconsultores.com)