

# El proyecto de adecuación a la LOPD de la Oficina Española de Patentes y Marcas

## Carlos Turmo Blanco

Director de la División de Tecnologías de la Información, Oficina Española de Patentes y Marcas

## Félix Serrano Delgado

Coordinador de Sistemas y Desarrollo Oficina Española de Patentes y Marcas

Esta comunicación se adscribe al punto 4 del temario del TECNIMAP 2010 "**Iniciativas legales y tecnológicas**", y en particular al apartado *Derechos de los ciudadanos en materia de Administración Electrónica y de protección de datos personales*. Escrito en Madrid, a 19 de febrero de 2010.

## 1 Introducción

El artículo 18.4 de la constitución dice que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".


Con la intención de hacer realidad este artículo, nace la Ley Orgánica 5/1992 conocida como LORTAD, para posteriormente ser derogada por la vigente Ley Orgánica de Protección de Datos de Carácter Personal, la LOPD (Ley Orgánica 15/1999).

La [Ley Orgánica de Protección de Datos \(LOPD\)](#), a través de sus 49 artículos, 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*".

El BOE de 21 de diciembre, aprueba el [Reglamento de desarrollo de la Ley Orgánica 15/1999](#) tanto de los ficheros automatizados como no automatizados que contengan datos de carácter personal. Este Reglamento tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados y no automatizados, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Esta ley se aplica a todos los profesionales, empresas y organizaciones públicas o privadas que almacenen, utilicen o traten datos de carácter personal registrados en soporte físico y que los haga susceptibles de tratamiento. Por tanto, aplica a la totalidad de las empresas

E-mail	<input type="text"/>
Clave	<input type="text"/>
DNI	<input type="text"/>
Nombres	<input type="text"/>
Apellidos	<input type="text"/>
Sexo	<input checked="" type="radio"/> Hombre <input type="radio"/> Mujer
Profesion	<input type="text"/>
Empresa	<input type="text"/>
Fecha de Nacimiento	<input type="text"/> Día <input type="text"/> Mes <input type="text"/> Año
Teléfono	<input type="text"/>
Dirección	<input type="text"/>
Ubicación Geográfica	<a href="#">Haga click aquí</a>
Nacionalidad	<input type="text"/>



**Datos de carácter personal:**  
cualquier información  
concerniente a personas  
físicas identificadas o  
identificables (LOPD,  
artículo 3)

(datos de clientes, proveedores, trabajadores, etc.).

En este documento se describe el Proyecto de adecuación a la LOPD, que la OFICINA ESPAÑOLA DE PATENTES Y MARCAS (en adelante, OEPM) decidió abordar en 2009 para el cumplimiento de lo dispuesto en la Ley Orgánica de Protección de Datos de Carácter Personal y en el Reglamento de Medidas para el desarrollo de la LOPD.

## 2 Antecedentes

La [OEPM](#) es un organismo autónomo, regulado por el [Real Decreto 1270/1997, de 24 de julio](#), y adscrito al [Ministerio de Industria, Turismo y Comercio \(MITYC\)](#) a través de la Subsecretaría (RD 1182/2008 de 11 de julio). La OEPM impulsa y apoya el desarrollo tecnológico y económico otorgando protección jurídica a las distintas modalidades de **Propiedad Industrial** mediante la concesión de *patentes y modelos de utilidad* (invenciones); *diseños industriales* (creaciones de forma); *marcas y nombres comerciales* (signos distintivos) y *títulos de protección de las topografías de productos semiconductores*. Asimismo, difunde la información relativa a las diferentes formas de protección de la propiedad industrial. En el plano internacional, la OEPM es la encargada de representar a España en los distintos foros y organizaciones internacionales que se encargan de la propiedad industrial e intelectual.

En el momento de escribir este artículo, la sede de la OEPM se encuentra ubicada en un edificio cercano al Paseo de la Castellana de Madrid, donde trabajan cerca de 800 personas. Por la naturaleza de sus funciones, la OEPM maneja habitualmente datos de carácter personal, afectados por tanto por la LOPD.

Desde la promulgación de la LOPD en 1999, la OEPM ha venido realizando las pertinentes publicaciones de los ficheros afectados por la LOPD en el BOE e incorporándolos al registro de la [Agencia Española de Protección de Datos](#) (donde figuran un total de [catorce ficheros](#) inscritos). Así, se han venido publicando en el BOE las sucesivas declaraciones de ficheros afectados por medio de la [Orden CTE/1986/2002, de 16 de julio](#), la [Orden CTE/2988/2003, de 14 de octubre](#), la Orden ITC/1977/2006, de 15 de junio, la Orden ITC/1864/2007, de 6 de junio y la [Orden ITC/2248/2009, de 31 de julio](#).

Hasta la fecha, estas actuaciones se han venido realizando por parte del Departamento de Coordinación Jurídica de la OEPM, en colaboración con la División de Tecnologías de la Información. Además se trabaja en cooperación con los departamentos encargados dentro de la Subsecretaría del MITYC.

## 3 Necesidades

¿No es suficiente con declarar los ficheros afectados en la Agencia y publicarlos en el BOE?  
¿Hay que hacer algo más?

En primer lugar, resulta conveniente realizar una labor exhaustiva de descubrimiento y consolidación de ficheros afectados, pues es posible que las sucesivas declaraciones de ficheros, a medida que iban siendo detectados, hayan omitido alguno de ellos, especialmente en aquellos casos en que se trate de ficheros en formato papel (no electrónicos), que sin embargo están igualmente protegidos por la LOPD.

Pero el cumplimiento de la LOPD es bastante más que las declaraciones. En concreto, es necesario asegurarse de que la información se maneja correctamente, y que las personas autorizadas para su tratamiento son conscientes de las responsabilidades legales asociadas. Es preciso que existan unos procedimientos adecuados, debidamente

documentados, para el manejo de la información. Debe existir un Responsable de Seguridad y debe existir un Documento de Seguridad. En definitiva, hay que poner los medios apropiados para el manejo de los Datos de carácter personal, de la forma que ha sido especialmente detallada en el Reglamento, publicado a finales de 2007.

Además hay que asegurar que se respetan los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en todos los puntos del proceso de manejo de datos personales. También, el Reglamento establece la obligación, a partir del nivel medio, de someter los sistemas de información e instalaciones de tratamiento y almacenamiento de, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad.

Aunque las AAPP no pueden ser sancionadas económicamente por el incumplimiento de la LOPD, sí que existen responsabilidades y consecuencias derivadas de las infracciones cometidas por las AAPP:

#### **Artículo 46. Infracciones de las Administraciones públicas.**

*1. Cuando las infracciones fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.*

*2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.*

*3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.*

*4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.*

A las necesidades intrínsecas anteriormente expresadas, se debe añadir la consideración de dos de los grandes marcos tecnológicos y de servicios en los que trabaja actualmente la OEPM:

- Establecimiento paulatino de un conjunto de buenas prácticas para la mejora de la **Calidad de los servicios TI**, tanto internos como externos, apoyada fundamentalmente en la [Biblioteca de Infraestructura de Tecnologías de Información](#), frecuentemente abreviada como ITIL.
- Adopción de un [Sistema de Gestión de la Seguridad de la Información](#) (SGSI) enmarcado dentro del estándar ISO 27001, y particularmente en la implantación de las obligaciones derivadas del [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](#).

## 4 Objetivos

Así pues, el Proyecto de Adecuación a la LOPD en la Oficina Española de Patentes y Marcas nace con los siguientes objetivos:

- Descubrimiento de ficheros afectados por la LOPD, tanto si ya están declarados como si aún no lo estuviesen.
- Diagnóstico de adecuación a la LOPD para los ficheros descubiertos en la fase de Consultoría, automatizados y no automatizados.

- Elaboración de medidas correctoras sobre las No Conformidades identificadas en el levantamiento de situación.
- Creación del Documento de Seguridad y los Procedimientos asociados para el manejo de la información afectada por la LOPD.
- Posible corrección de las inscripciones en el registro de ficheros de la Agencia Española de Protección de Datos, y correspondientes publicaciones en el BOE, en su caso.
- Realización de la primera Auditoría LOPD, que se debe repetir con carácter bienal según obliga el Reglamento de la LOPD.

## 5 Alcance

Tal y como ya se ha adelantado, se han contemplado distintos escenarios de análisis en función de la localización de los datos objeto de la consultoría. Por un lado, se procede a revisar todos los datos propiedad de la OEPM, que pueden estar almacenados en Sistemas de información y las Bases de Datos Corporativas en las instalaciones de la OEPM, o bien almacenados en ficheros en los ordenadores de los propios usuarios de la OEPM, así como otros posibles conjuntos de datos custodiados por un tercero (posiblemente alojados en instalaciones externas) y regulados bajo acuerdo de Nivel de Servicio.

Por otro lado, se contemplan todos los posibles datos, que pueden estar almacenados en distintos soportes, tanto en formato electrónico como en papel.

## 6 Desarrollo del Proyecto

El proyecto, una vez concebido, se desarrolla según las fases que se describen en los sucesivos apartados de este epígrafe.

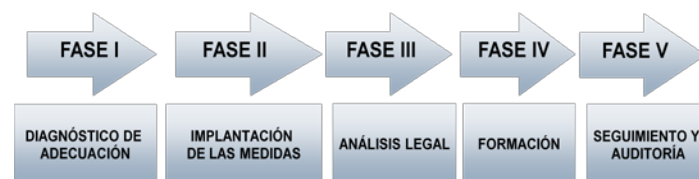
En el momento de escribir este artículo (Febrero de 2010), ha concluido todas las fases de diseño del proyecto, constitución del equipo de trabajo, levantamiento de la situación, confección y entrega del informe y recomendaciones, estando actualmente terminando la fase de diseño del Plan de Acción.

En los próximos meses está prevista la conclusión del resto de las fases del Proyecto.

### 6.1 Diseño del proyecto

En la fase de diseño se procedió a establecer los principios enumerados anteriormente, así como a determinar los correspondientes actividades a realizar, incluida la contratación de parte de los trabajos a una empresa especializada.

En la fase de diseño se procedió también a la adopción de la *metodología* a utilizar durante el desarrollo de los trabajos y a elaborar un *Plan de trabajo*.



**Ilustración 1: Metodología empleada en el Proyecto**

Los trabajos se planificaron para su desarrollo a lo largo de dos meses, según se refleja en el cronograma del proyecto.

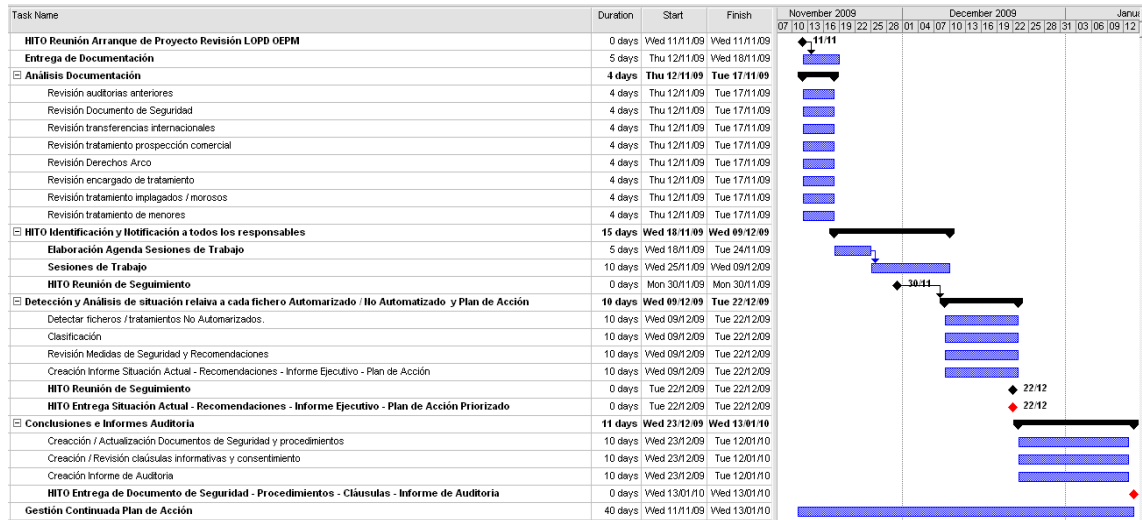


Ilustración 2: Plan de Trabajo del Proyecto

## 6.2 Presentación a la Dirección

Debido a la naturaleza de éste proyecto, que afecta a toda la organización, y en aspectos que en algunos casos pueden ser particularmente sensibles, ha sido presentado al *Comité de Dirección de la OEPM*, con el doble objetivo de dar a conocer el proyecto a todas las Unidades, así como recibir el apoyo explícito de la Dirección, lo cual ha facilitado grandemente el desarrollo de los trabajos.

## 6.3 Constitución del Equipo de Trabajo

Como primera tarea efectiva, se procedió a dar inicio al proyecto y a constituir el equipo de trabajo, compuesto por un Director de Proyecto perteneciente a la OEPM, un representante de la DTI que coordinaba todos los aspectos tecnológicos de los Sistemas de Información de la OEPM, un representante del Departamento Jurídico de la OEPM, y por parte de la empresa colaboradora, un Jefe de Proyecto, acompañado por los correspondientes Consultores y especialistas, todo ello supervisado por el correspondiente Control de Calidad.



Ilustración 3: Equipo de Proyecto

## 6.4 Levantamiento de la Situación

En esta fase se ha procedido, por medio fundamentalmente de entrevistas, a revisar las posibles existencias de ficheros afectados en todas y cada una de las Unidades Administrativas de la OEPM, y a verificar el estado de cumplimiento de cada uno de ellos. Las Unidades participantes fueron:

Unidades de la OEPM entrevistadas sobre posibles archivos afectados por la LOPD

Departamento de Signos Distintivos

Departamento de Patentes e Información Tecnológica

Departamento Jurídico y de Relaciones Internacionales

División de Tecnologías de la Información

Secretaría General

Unidad de Apoyo a la Dirección de la OEPM

Vocalía de Calidad

## 6.5 Entrega del informe de situación y las recomendaciones

Como resultado de los trabajos efectuados, se ha elaborado un documento que refleja el grado de adecuación a la LOPD de la OEPM. En éste informe se revisan, fichero a fichero, y medida a medida, el grado de adecuación, calificándose con uno de entre tres posibles valores de conformidad a la LOPD:



### **Conformidad: No Conforme.**

*La medida se encuentra poco o nada implantada pudiéndose obtener un impacto negativo en la organización. Este no cumplimiento puede ser originado por alguno de los siguientes motivos:*

- *Se ha detectado un grado de cumplimiento nulo o poco significativo de las áreas de las organizaciones.*
- *El grado de cumplimiento es aislado, por iniciativa personal o departamental, pero no a nivel global en la compañía.*
- *La medida no está implantada en la organización ni se había detectado esta necesidad.*



### **Conformidad: Conforme Parcialmente.**

*Existe una implantación parcial de las medidas que hacen cumplir en parte el grado de adaptación a la LOPD en la organización, pero no cubre adecuadamente los requisitos especificados en la ley por diversos motivos, tales como por ejemplo:*

- *Falta de tiempo.*
- *Desconocimiento de las medidas a aplicar.*
- *Complejidad operativa del proceso.*





**Conformidad: Conforme.**

*El grado de cumplimiento es óptimo y los procesos están implantados completamente cumpliendo con la legislación aplicable en cuanto a LOPD se refiere.*

Para cada uno de los ficheros examinados se entrega un inventario categorizando los siguientes aspectos:

- Nivel de clasificación del fichero (Bajo/Medio/Alto)
- Responsable del fichero
- Responsable del tratamiento
- Información personal que contiene el fichero
- Mecanismo utilizado para la captación de los datos
- Soporte utilizado para su almacenamiento
- Transferencias Internacionales
- Tratamiento de Terceros
- Entidades u Organismos a los que se ceden datos contenidos en el fichero
- Personal que tiene acceso a la información

En cada uno de los aspectos analizados, cuando es de aplicación, se incorporan además un conjunto de recomendaciones, que permiten remediar o mejorar el cumplimiento de la LOPD en ese aspecto. Así por ejemplo, se muestra el resultado concerniente a los ficheros temporales utilizados en las aplicaciones y sistemas afectados por la LOPD:

### ***Ficheros Temporales***

*Los ficheros temporales deben cumplir el mismo nivel de seguridad que les corresponda con arreglo a los criterios señalados en el Reglamento, y deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación.*

#### **Situación Actual**

*El personal de los equipos informáticos que manejan datos de carácter personal en la Oficina Española de Patentes y Marcas sabe que deben borrar este tipo de información una vez que ha finalizado el proceso para el que fue creada. Los usuarios no conocen sus obligaciones en relación con los ficheros temporales. No existe un procedimiento escrito y comunicado de gestión de ficheros temporales.*

#### **Recomendaciones**

*Ha de existir un procedimiento de gestión de ficheros temporales, en el cual se indique que los ficheros temporales deben ser borrados cuando ya no son necesarios. (El concepto de "ficheros temporales" incluye, además de los propios generados por una aplicación que trate datos de carácter personal, las copias que se hagan para usos puntuales de este tipo de información).*

*Este procedimiento será conocido por todo el personal de la Oficina Española de Patentes y Marcas que trate datos de carácter personal.*



**Conformidad: No Conforme**

El conjunto de aspectos analizados ha sido muy numeroso, pero entre ellos podemos destacar especialmente los siguientes:

- Consentimiento del Afectado y Derecho de Información en la Recogida de los Datos

- Responsable del Fichero
- Cesión de Datos y Acceso por Cuenta de Terceros
- Derecho de Acceso, Rectificación, Cancelación y Oposición
- Creación, Modificación o Supresión de Ficheros
- Documento de Seguridad
- Funciones y Obligaciones del Personal
- Registro de Incidencias
- Identificación y Autenticación
- Control de Acceso
- Gestión y Distribución de Soportes
- Copias de Respaldo y Recuperación
- Responsable de Seguridad
- Registro de Accesos

El documento se organiza en capítulos que comprenden la relación de los ficheros afectados, la aplicación de los principios de la protección de los datos de carácter personal, las medidas de seguridad aplicadas a los ficheros automatizados y las medidas de seguridad aplicadas a los ficheros no automatizados.

## 6.6 Elaboración del Plan de Acción

En esta fase, y a la vista de las conclusiones y recomendaciones de la fase de levantamiento de la situación, se diseñan un conjunto de acciones a tomar, entre ellas:

- Elaboración del Documento de Seguridad y otros documentos de apoyo
- Revisión de la inscripción en la AGPD de los ficheros de la OEPM
- Planes de formación y divulgación específica de la LOPD en la OEPM
- Desarrollo de otras posibles medidas técnicas y organizativas
- Auditoría de Seguridad

## 6.7 Elaboración del Documento de Seguridad y otros documentos de apoyo

El documento de Seguridad incluye las medidas y procedimientos de cumplimiento común y obligado para todos los sistemas, así como la estrategia general de seguridad a adoptar. Entre ellas:

- Funciones y obligaciones
- Registro de incidencias
- Telecomunicaciones
- Identificación y autenticación
- Control de acceso
- Gestión de soportes
- Copias de seguridad
- Pruebas con datos reales
- Requisitos de desarrollo de aplicaciones

Además, se elaboran otros documentos de apoyo para el cumplimiento de la LOPD, como pueden ser los siguientes:

- Cláusulas tipo relativas a la utilización de datos personales en los contratos que la OEPM celebre, para que se adecuen a los artículos 5 (recogida de datos) y 6 (consentimiento del afectado) de la LOPD en cuanto a qué información hay que



proporcionar en la recogida de datos personales y cómo se ha de recoger el consentimiento del afectado para su tratamiento por parte de la OEPM, en todos aquellos canales en los que dicha recogida se pueda llevar a cabo.

- Instrucciones de inclusión de los derechos ARCO en los formularios (en papel o electrónicos) que la OEPM pueda ofrecer a los usuarios y que estén afectados por la LOPD.

## 6.8 Revisión de la inscripción en la AGPD de los ficheros de la OEPM y otras actuaciones legales

**Revisión de la inscripción en la AGPD:** Actualmente la OEPM tiene inscritos 14 ficheros en la APD. Se procederá a la revisión de dichas inscripciones, verificando la actualidad de los datos inscritos, y se procederá a su modificación o cancelación si fuera necesario ante la APD. De igual modo, se revisarán los ficheros que manejen datos personales y se procederá a comprobar si la actual inscripción los tiene contemplados. Si no fuera así se procederá a su alta en el Registro General de Protección de Datos de la APD.

**Revisión de la prestación de servicios y de las cesiones de datos:** Tal y como se regula la Prestación de Servicios en el artículo 12 de la LOPD y la comunicación de datos (anteriormente cesión) en el artículo 13 de la LOPD, es necesario que los intercambios de datos personales entre la OEPM y otras entidades estén regulados de forma contractual, y que en dichos contratos se incorporen las cláusulas pertinentes que regulen el tratamiento de los datos en caso de la prestación de servicios y de la comunicación de datos a terceros. En esta tarea se revisarán los contratos y las relaciones actuales entre la OEPM y otras entidades.

**Revisión de los procesos internos de comunicación:** La LOPD regula en su artículo 15 el derecho de acceso por parte de los afectados (personas de las que disponemos datos personales) a los datos que se manejen por parte de la empresa, dando a la empresa un plazo de contestación a las peticiones de acceso de 1 mes. Por otra parte, en el artículo 16 de la LOPD se regula el derecho de Rectificación y Cancelación de datos personales por parte del afectado, dando a la empresa en este caso un plazo de 10 días para que haga los cambios pertinentes en sus sistemas. El objetivo de esta tarea es revisar los flujos internos de tratamiento de datos y los procedimientos de ejecución de los derechos de los afectados, optimizándolos para cumplir los plazos legales.

## 6.9 Divulgación y Formación

Tras haber completado las anteriores fases del proyecto y de haber presentado los resultados obtenidos, se debe proceder a la divulgación del Proyecto LOPD y de las cuestiones concretas que afectan a los usuarios en la OEPM.

Para llevar a cabo dicha divulgación, se van realizar jornadas divulgativas dirigidas a los diferentes estamentos de la organización, teniendo en cuenta las distintas responsabilidades que cada nivel tiene sobre el tratamiento de datos personales.

Estas acciones de comunicación cubrirán también aspectos de concienciación de las personas en el tratamiento de los datos personales, funciones y responsabilidades en el tratamiento de datos personales identificadas en los documentos de seguridad, responsables del fichero y medidas de seguridad implantadas en los sistemas de información como resultado del proyecto.

Las acciones divulgativas también prevén emplear para el colectivo de usuarios la utilización de murales, trípticos, o material similar.

Además se ha previsto una acción formativa específica en LOPD, combinada con la formación en Seguridad de la Información, e integrada en el Plan de Formación de la OEPM para 2010, con el siguiente programa formativo.

## Seguridad TI

La Seguridad Integral de los Sistemas de Información.  
Marco Jurídico de la Seguridad de los Sistemas de Información.  
Aspectos Básicos de la Seguridad de Información.  
Los Responsables de la Seguridad.  
Clasificación de los Activos de Información.  
Estrategias y Políticas de Seguridad.  
Análisis y Gestión de Riesgos.  
Normas, Procedimientos y Planes de Contingencias.  
Medidas para la Seguridad Física.  
Medidas para la Seguridad Lógica.  
Medidas de Protección Administrativas, Organizativas y Legales.  
Estándares sobre la Seguridad de los Sistemas de Información.  
El Documento de Seguridad. Auditoría de la Seguridad Informática.  
Informática Forense.

## LOPD

Introducción a la protección de datos de carácter personal  
Definiciones de la LOPD y su Reglamento de desarrollo  
Principios en materia de protección de datos de carácter personal  
Derechos de los afectados  
Los Ficheros de Titularidad Pública  
Medidas de seguridad  
Infracciones y sanciones  
La Agencia de Protección de Datos

## 6.10 Informe de Auditoría

**Auditorías:** En esta fase se realiza la auditoría para verificar el cumplimiento de las recomendaciones efectuadas en el Dictamen Preliminar y el Documento de Seguridad. Según se indica en los artículos 15 y 17 del Real Decreto 995/1999, se deben establecer y realizar auditorías de seguridad como mínimo cada dos años y una serie de controles de carácter periódico, para verificar el cumplimiento de lo estipulado en el Documento de Seguridad, y se deben llevar a cabo auditorías de adecuación y cumplimiento de las medidas de seguridad definidas en dicho documento.

Por ello, y una vez ejecutados los diferentes Planes de acción, se debe proceder a la verificación mediante auditoría y al establecimiento del Manual de Procedimiento de Auditoría de Seguridad. Como resultado de las auditorías se realizará un Informe de Auditoría de Seguridad.

El **Informe de Auditoría de Seguridad** debe cubrir los siguientes puntos:

- Metodología y plan de trabajo desarrollado.
- Aspectos contemplados en la auditoría.
- Cumplimiento de las medidas requeridas en cada uno de ellos.



- Síntesis de las no conformidades o carencias detectadas.
- Propuesta de acciones correctoras y de mejora.
- Conclusiones

A modo de ejemplo ilustrativo un posible índice del **Informe de auditoría** sería:

- Objetivo, Alcance y Limitaciones
- Documento de Seguridad: medidas técnicas / organizativas
- Estructura de los Sistemas y Aplicaciones que tratan datos de carácter personal
- Funciones y Obligaciones
- Conclusiones: Fortalezas, Debilidades y Puntos de Atención
- Estado Actual de los Sistemas / aplicaciones
- Procedimiento de Recuperación de Datos
- Controles de Verificación
- Aspectos Jurídicos: Modificaciones a los ficheros inscritos en la Agencia de Protección de Datos
- ANEXO I - Matriz de Resultados de la Auditoría
- ANEXO II - Resumen de Tareas Pendientes y Recomendaciones

## 7 Beneficios del proyecto

### Cumplimiento de las obligaciones legales

Como consecuencia de la ejecución de este proyecto y del alcance de sus objetivos, se obtendrán además una serie de beneficios. El primero y más obvio es el cumplimiento con lo dispuesto en la Ley Orgánica de Protección de Datos. Se debe recordar que la LOPD es de obligado cumplimiento, tanto para la Administración Pública como para las empresas.

### Mejora del servicio y de la imagen de la OEPM

Además, gracias a los procesos ordenados en el manejo de datos de carácter personal existen mejoras en la respuesta ante incidentes de seguridad, generando fortalezas para la administración pública, y por consiguiente logrando generar mayor confianza para la ciudadanía. Esta fortaleza ayudará además a resolver satisfactoriamente posibles situaciones de desprestigio en las administraciones públicas, como podría ser que alguien extraiga ilegalmente datos para obtener beneficios económicos o de otro tipo, o posibles incidentes en caso de imprevistos como incendios e inundaciones que afecten a los Sistemas de Información y a las Bases de Datos.

### Ahorro económico

Por otra parte se consigue un importante ahorro económico potencial, evitando pérdidas económicas en concepto de responsabilidad civil, al haber asegurado los datos de los interesados. Incluso, las medidas de protección destinadas a guardar los datos en repositorios seguros nos permitirán recuperar el ritmo de trabajo inmediatamente, con el consiguiente ahorro de costes, y sin daños para la imagen de la OEPM.

### Implantación del Esquema Nacional de Seguridad

El proyecto de adecuación a la LOPD tiene también un efecto de *punta de lanza* como primer paso para atender las obligaciones derivadas del Esquema Nacional de Seguridad, que dice, en su Artículo 11:

#### **Artículo 11. Requisitos mínimos de seguridad.**



1. Todos los órganos superiores de las Administraciones públicas **deberán disponer formalmente de su política de seguridad**, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

*Organización e implantación del proceso de seguridad.*

*Análisis y gestión de los riesgos.*

*Gestión de personal.*

*Profesionalidad.*

*Autorización y control de los accesos.*

*Protección de las instalaciones.*

*Adquisición de productos.*

*Seguridad por defecto.*

*Integridad y actualización del sistema.*

*Protección de la información almacenada y en tránsito.*

*Prevención ante otros sistemas de información interconectados.*

*Registro de actividad.*

*Incidentes de seguridad.*

*Continuidad de la actividad.*

*Mejora continua del proceso de seguridad.*

## Calidad en la OEPM

El cumplimiento de la normativa de protección de datos personales supone, por fin, ofrecer una imagen de control, eficacia y orden de los documentos y datos que fluyen por la administración pública. Esto reforzará el resto de **procesos de calidad de la gestión de la OEPM**. No olvidemos que la OEPM está implicada en una política de calidad, que figura expresamente en su propio sitio web <http://www.oepm-calidad.es> y ha obtenido y mantiene el *certificado ISO9001:2000 para el Proceso PCT y los Servicios de Información Tecnológica*, y la *Certificación del Sistema de Vigilancia Tecnológica del Servicio de Búsquedas según norma UNE166006:2006 EX* (gestión de la I+D+I).

## 8 Conclusiones

Aunque éste proyecto se concibe con una estructura clásica (inicio, diseño, ejecución y conclusión) no cabe duda que, al tratarse de procesos vivos, las labores de vigilancia y adecuación a la LOPD han de ser constantes y permanentes.

Por otra parte, en un proceso como éste que abarca a toda la organización, contar con el apoyo expreso de la Dirección desde el principio es fundamental para que alcance sus objetivos.

Finalmente, los aspectos de seguridad y calidad de los servicios parece que serían los primeros candidatos a sufrir recortes en un contexto de crisis como el actual. Por ello es especialmente importante resaltar los beneficios obtenidos, así como las obligaciones legales a las que las AAPP por su naturaleza están especialmente obligadas a respetar.

## 9 Agradecimientos

Deseo expresar mi agradecimiento a por su aportación y colaboraciones a éste proyecto y para la redacción de éste artículo a todo el personal de la OEPM que colabora en éste proyecto, así como a la empresa ATOS ORIGIN, que actualmente trabaja contratada por la OEPM realizando los trabajos de consultoría necesarios para la adecuación a la LOPD.