



# **NUEVA APLICACIÓN DE GESTIÓN ELECTRÓNICA EN PROTECCIÓN DE DATOS DEL MINISTERIO DE TRABAJO E INMIGRACIÓN**

**DIRECCIÓN GENERAL DE SERVICIOS  
SUBDIRECCIÓN GENERAL DE PLANIFICACIÓN Y  
COORDINACIÓN INFORMÁTICA  
Área de Comunicaciones y Seguridad**

**Autores: María José Lucas Vegas - Consejera Técnica  
Guillermo B. Mora Marín - Jefe de Proyecto de Sistemas Informáticos**

## 1 Introducción

En 1999, se promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), que más tarde fue parcialmente desarrollada por el 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.

Esta normativa plantea a los responsables de un fichero de datos de carácter personal, entre otras, las siguientes obligaciones en materia de protección de datos:

- Notificar a la Agencia Española de Protección de Datos (en adelante, AEPD) la existencia de ficheros de datos personales, así como diferente información relacionada con dicho fichero (estructura, nivel de seguridad, cesiones previstas, transferencias internacionales, etc).
- Deber de informar a los interesados de la existencia de un fichero o tratamiento de datos, de la finalidad de la recogida de éstos, etc.
- Hacer efectivos los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) de los interesados cuando el interesado así lo requiera en aquellos casos recogidos por la ley.
- Aplicación de las medidas de seguridad establecidas por el mencionado reglamento atendiendo al nivel de seguridad asociado a los ficheros, ya sean manuales o no o de tipo mixto. Entre estas medidas tendríamos la creación del documento de seguridad y su mantenimiento y actualización
- Realización de auditorías, al menos, para los ficheros de nivel medio o alto.
- Establecimiento, en su caso, de las obligaciones a satisfacer por los encargados del tratamiento de ficheros de datos personales por cuenta del responsable.

Por otro lado el Ministerio de Trabajo e Inmigración (en adelante MTIN) es un Departamento grande donde tenemos como unidades responsables de ficheros las siguientes (aproximadamente):

- 95 en Servicios Centrales, se incluyen las Entidades Gestoras, los Organismos Autónomos, etc.
- 300 a nivel provincial, Inspecciones Provinciales de Trabajo y Seguridad Social, Direcciones Provinciales de las Entidades Gestoras de la Seguridad Social, Centros de Sanidad Marítima, Centros Nacionales de Formación Marítima, Escuelas de Formación Profesional Marítimo-Pesqueras, Servicios Jurídicos Delegados Provinciales, etc.
- 35 a nivel internacional, Consejerías y Secciones Laborales y Centros Asistenciales del ISM.

Atendiendo a su nivel de seguridad la distribución de los ficheros sería aproximadamente:

- 90 ficheros de nivel alto
- 120 ficheros de nivel medio
- 1020 ficheros de nivel básico

En cuanto al volumen actual de ficheros de datos de carácter personal, el Departamento tiene declarados en la AEPD 1300 ficheros aproximadamente, lo cual

supone aproximadamente el 28% de todos los ficheros declarados a nivel nacional en la AEPD (actualmente unos 4500 ficheros). El Departamento publica, en general, dos órdenes ministeriales al año para crear modificar o suprimir ficheros de datos de carácter personal.

En la siguiente tabla podemos ver algunas de las disposiciones publicadas desde el



año 2008:

## 1 Proceso de notificación de ficheros del Departamento a la AEPD

Las unidades responsables de ficheros en el Departamento cuando quieren notificar un alta, una modificación o una supresión de un fichero en el Registro General de la Agencia Española de Protección de Datos envían un oficio y su formulario Nota asociado a la Subdirección General de Planificación y Coordinación Informática, que es la unidad competente dentro del Departamento para realizar todo el proceso de elaboración y gestión del proyecto de orden ministerial, así como la notificación a la AEPD; tan pronto se publica la disposición en el Boletín Oficial del Estado (en adelante BOE).

La notificación de los ficheros a la Agencia se realizaba fichero a fichero, cumplimentando previamente los datos del declarante de forma manual con un navegador.

Existe una base de datos Notes que ha sido utilizada para dar a conocer a través de la Intranet del Departamento los ficheros de datos notificados por el MTIN a la AEPD, así como para generar el anexo de la Orden Ministerial correspondiente, aunque todo este proceso se realizaba de forma manual.

Con el fin de agilizar la gestión interna de la Órdenes Ministeriales, mejorar la información ofrecida a las unidades responsables de los ficheros a través de la Intranet y proporcionar una aplicación de soporte a las unidades responsables de los ficheros en materia de protección de datos, la Subdirección General de Planificación y Coordinación Informática, ejerciendo la competencia establecida en el artículo 12 apartado c, del Real Decreto 1129/2008, de 4 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo e Inmigración y se modifica el Real Decreto 438/2008, de 14 de abril, por el que se aprueba la estructura orgánica básica de los departamentos ministeriales, " *la gestión de las medidas previstas en materia de protección de datos de carácter personal,*" ha licenciado y adaptado una aplicación DPC/Sistema de Protección de Datos Personales, suministrada por la empresa Sistemas Informáticos Abiertos S.A.(SIA) que facilitará el cumplimiento de la normativa de protección de datos en el ámbito del Ministerio de Trabajo e Inmigración. La aplicación se denominará dentro del ámbito del Departamento Aplicación LOPD.

En los siguientes apartados se describen las funcionalidades de la aplicación y en qué medida pueden:

- Ayudar a los responsables de ficheros a satisfacer las obligaciones establecidas

en la normativa de protección de datos:

- Derechos ARCO
  - Encargado del Tratamiento
  - Derecho de Información
  - Medidas de seguridad y auditorías asociadas, en su caso.
  - Notificación de ficheros en la AEPD
  - Control de las cesiones realizadas
- Agilizar el proceso de declaración de los ficheros en la AEPD.
  - Publicación de toda la documentación de interés en materia de protección de datos.

## 1 Descripción de la Aplicación

A continuación se describen las principales funcionalidades de la aplicación de gestión de la LOPD. El aspecto inicial de la aplicación es el siguiente:

Rol	Sis. Información	Auditoría	Fecha Ini.
gestor del archivo	SI.SG DE PLANIFICACION Y COORDINACION INFORMATICA-ALTO	SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA (Título VIII RD 1720/2007)	08/03/2010
Técnico adm. calificado	SI.SG DE PLANIFICACION Y COORDINACION	SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION	08/03/2010

Pregunta	Usuario	Contestada
¿Existe un registro de entrada de soportes informáticos?	gboram	<input type="checkbox"/>
Las personas que realizan la recepción de soportes informáticos con datos de carácter personal, están debidamente autorizadas en el documento de seguridad?	gboram	<input type="checkbox"/>

Rol Rechazado	Tipo Rechazo	Texto Rechazo
SI.aaa - SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA (Título VIII RD 1720/2007)		
Técnico de backups	Desconocimiento	desa
Técnico de desarrollo	Reasignación	lkj
Utilizador	No seleccionado	no
SI.aaa - SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA (Título VIII RD 1720/2007)		

Recomendación	Auditoría	Fecha Ini.	Fecha Tope
---------------	-----------	------------	------------

donde podemos ver el panel que se encuentra el usuario al acceder. Vemos las cuatro pestañas con las funcionalidades de la aplicación y cuatro paneles con las tareas pendientes del usuario. Solo se muestran al usuario las pestañas a las que está autorizado y solo tiene acceso a los datos de su entorno de trabajo.

A continuación se muestran todas las opciones posibles en los menús:

FUNCIONALIDADES DE LA HERRAMIENTA DE GESTIÓN DE LA LOPD							
<b>Gestión</b>		<b>Adecuación</b>		<b>Auditoría</b>		<b>Informes</b>	
<b>Biblioteca</b>	Categorías	<b>Notificación de ficheros</b>	Gestión de notificaciones	<b>Sistemas de información</b>		<b>Informes de adecuación</b>	Documentación formal de Adecuación
	Documentos		Gestión de Envíos	<b>Gestión de auditorías</b>			Información pública de ficheros inscritos
<b>Marco normativo</b>	Marco jurídico	<b>Disposiciones de carácter general</b>		<b>Formularios</b>		<b>Informes de auditoría</b>	
	Artículos	<b>Ejercicio de derecho (ARCO)</b>		<b>Gestión de recomendaciones</b>	Consulta de recomendaciones	<b>Biblioteca de documentos</b>	
	Puntos de control	<b>Documento de seguridad</b>	Generación/Modificación		Gestión de recomendaciones	<b>Consulta de documentos de seguridad</b>	Ámbito público
	Recomendaciones		Acciones delegadas	Asignación de recomendaciones	Ámbito ARCO		
<b>Unidades organizativas</b>		<b>Cumplimiento de principios legales</b>	Derecho de Información y Consentimiento. Art. 5 y Art.6	<b>Registro de incidencias</b>		Ámbito Soportes	
<b>Perfiles y usuarios</b>	Perfiles		Comunicación de datos. Art.11				
	Usuarios	Encargado de Tratamiento Art 12	Soportes de entrada				
<b>Ficheros</b>	Consulta usuarios-perfiles	<b>Gestión de entrada y salida de soportes</b>	Soportes de salida			Ámbito Responsable de Fichero	
	<b>Configuración</b>	<b>Registro de incidencias</b>					

Entre todas las obligaciones y funciones que hemos de realizar para cumplir con la LOPD y su reglamento de desarrollo, las que pueden requerir más soporte por su complejidad son:

- Declaración de los ficheros ante la Agencia Española de Protección de Datos.
- Elaboración del Documento de Seguridad.
- Realización de Auditorías.

Las tres son contempladas en la aplicación, además de todas las demás, realizándose de la siguiente manera:

### 1.1 Declaración de los ficheros ante la Agencia Española de Protección de Datos.

En el caso de las Administraciones Públicas para realizar la gestión de inscripción ante la AEPD es necesario publicar antes una Disposición General con todos los ficheros que se quieren dar de Alta, Modificar o dar de Baja. La declaración de cada fichero se realiza en la siguiente pantalla:

Notificación de Ficheros

Modificar datos del Responsable del Fichero. Los campos marcados con asterisco (\*) son obligatorios. Tipo de administración a la que pertenece\*

ADMINISTRACIÓN GENERAL DEL ESTADO

Encuadre Administrativo del Órgano

Denominación del Ministerio/Consejería/Ayuntamiento o Entidad Local/Ente Público\* MINISTERIO DE TRABAJO E INMIGRACION Denominación Dirección General / Dependencia\* SUBDIRECCION GENERAL DE GESTION DE RR

Nombre del Órgano Responsable\* INSTITUTO NACIONAL DE LA SEGURIDAD SO

CIF del órgano de la Administración\* Domicilio Social / Apartado de Correos\* MADRID DAMIAN, 4-6

Localidad\* MADRID Código Postal\* MADRID 28036 Provincia\* MADRID País\* ESPAÑA

Teléfono\* 915444333 Fax\* 915444333 Correo Electrónico\*

**Derechos de acceso, rectificación, cancelación y oposición**

Modificar Responsable del Fichero

Nombre de la oficina o dependencia

Domicilio Social / Apartado de Correos

Localidad País Seleccione una opción

Teléfono Fax Correo Electrónico

**Encargado del tratamiento**

Modificar datos Encargado del Tratamiento

Nombre y apellidos o Razón Social

Dirección Postal

Localidad País Seleccione una opción

Teléfono Fax Correo Electrónico

**Identificación y finalidad del fichero**

Modificar Identificación y Finalidad del Fichero

Denominación

Descripción detallada de finalidad y usos previstos\*

donde completaríamos todos los datos que exige la AEPD para cada fichero. Una vez incluidos todos los ficheros o sus modificaciones pasaríamos a generar el proyecto de Disposición General y su seguimiento en la tramitación asociada hasta su

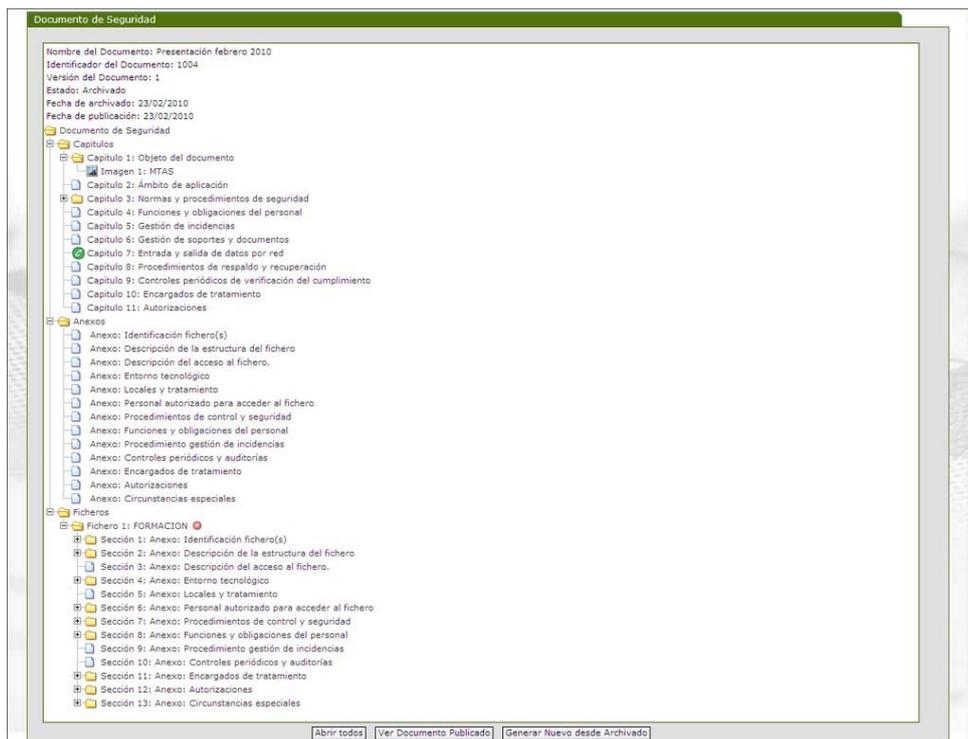
Nombre de Disposición	Diario oficial	Estado	Nº boletín	Fecha public.	Nº orden
DG PARA CREAR INFORME	BOE	En tramitación Pte. Mini...			
OM	BOE	Publicada	1	24/02/2010	1
OM PRUEBA FEB2010 FICHEROS FALLECIDOS	BOE	Publicada	1	17/02/2010	1
om prueba1	BOE	Publicada	1	08/03/2010	1
OMPRUEBA	BOE	Publicada			
OM01	BOE	Publicada	01	01/10/2009	1777
om02	BOE	Publicada	2	29/10/2009	2
om03	BOE	En tramitación Pte. Mini...	3	29/10/2009	3
OTRA PRUEBA	BOE	Publicada	3	02/03/2010	3

publicación en el BOE de publicación desde la siguiente pantalla:

después se realizaría el envío a la AEPD. Hasta ahora dicho envío era realizado por medio del formulario NOTA, fichero a fichero vía Internet. Ahora el envío de los ficheros es realizado de manera telemática desde la propia aplicación, pudiendo ser un envío firmado digitalmente con lo cual acabaría el proceso de notificación o con un envío sin firmar con lo que se generaría una hoja de envío que se haría llegar a la AEPD por correo ordinario.

## 1.2 Elaboración del Documento de Seguridad

Cada fichero con datos de carácter personal tiene que tener su correspondiente Documento de seguridad con las medidas y procedimientos de seguridad que se le aplican teniendo en cuenta tanto su nivel de seguridad como el tipo de tratamiento que se le aplica. La aplicación genera automáticamente el esqueleto del mismo con todos los requerimientos necesarios para que sea completo. A partir de este esqueleto debemos completar las medidas específicas aplicables al mismo incluyendo, cuando sea el caso, las evidencias o documentación que se estime necesaria. El Documento de Seguridad se cumplimenta en la siguiente pantalla:



donde se pueden observar todos los capítulos y anexos y una sección por cada fichero implicado ya que el mismo documento de seguridad se puede aplicar a más de un fichero si les da soporte el mismo Sistema de Información.

### 1.3 Realización de Auditorías

Según el Real Decreto 1720/2009 de desarrollo de la LOPD hay que realizar auditorías de las medidas de seguridad aplicadas a los ficheros con datos de carácter personal al menos cada dos años. Siendo la labor de auditoría larga y compleja, la aplicación nos permite simplificarla en gran manera y agrupar en un solo lugar todas las tareas a realizar, incluyendo la gestión de recomendaciones posteriores a la auditoría. En primer lugar hay que crear los Sistemas de Información que dan soporte a los ficheros y luego asignar a cada Sistema de Información los ficheros a los que da soporte, lo cual se hace en la siguiente pantalla:

Detalle Sistema Información

Nombre: SI.SG DE PLANIFICACION Y COORDINACION INFORMATICA.ALTO Descripción: Sistema de Información SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA Alto

Ubicación: SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION Nivel de seguridad: Alto

Gestor: Tipo de tratamiento: Parcialmente automatizado

Auditable:

**Ficheros**

Nombre	Tipo de tratamiento
PLAN DIRECTOR SISTEMAS INFORMACION	Automatizado

**Entidades Usuarías**

Nombre
SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION

**Asignación de Roles**

Rol	Perfil / Entidad
Conocedor	RF - Conocedor / SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA
Utilizador	RF - Utilizador / SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA
Técnico de desarrollo	RF - Técnico de desarrollo / SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA
Técnico de comunicaciones	RF - Técnico de comunicaciones / SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA
Técnico de sistemas	RF - Técnico de Sistemas / SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA

después, tras activar la auditoría, habrá que responder a una serie de formularios distribuidos por capacidades técnicas entre los usuarios que se consideren oportunos dentro de la organización, mostramos a continuación el de un técnico de

Formulario del sistema de información: SI.SG DE PLANIFICACION Y COORDINACION INFORMATICA.MEDIO / Auditoria: Título VIII RD 1720/2007 -- SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA -- 08/03/2010

Rol: Técnico de backups

Acción	Punto de control	Respuesta	Evidencia
<input checked="" type="checkbox"/>	RF - Técnico de backups - SUBDIRECCION GENERAL DE PLANIFICACION Y COORDINACION INFORMATICA		
<input checked="" type="checkbox"/>	¿Se hace un inventario de los documentos que contienen datos de carácter personal?	SI	⊗
<input checked="" type="checkbox"/>	Los documentos que contienen datos de carácter personal, ¿permiten identificar el tipo de información que contienen? En el momento que se requiere sea afirmativa, indicar cuál es el mecanismo de identificación utilizado (mediante etiquetas, otros) adjuntando, al tiempo que la evidencia, el documento en el que se encuentra reflejada o incorporada esta información.	SI	⊗
<input checked="" type="checkbox"/>	¿La identificación de los soportes con datos de carácter personal especialmente sensibles para la organización, se realiza utilizando sistemas de etiquetado comprensible y con significado que permitan al personal autorizado identificar su contenido?	SI	⊗
<input checked="" type="checkbox"/>	¿El etiquetado utilizado facilita la identificación de los soportes a personas que no se encuentran autorizadas para acceder a ellos?	No	⊗
<input checked="" type="checkbox"/>	¿Se hace un inventario de los soportes que contienen datos del sistema de información?	No	⊗
<input checked="" type="checkbox"/>	¿Está justificado debidamente en el documento de seguridad los motivos por los que no se encuentran inventariados los soportes que contienen datos de carácter personal?	No	⊗
<input checked="" type="checkbox"/>	¿Está justificado debidamente en el documento de seguridad los motivos por los que no se encuentran inventariados los soportes que contienen datos de carácter personal?	SI	⊗
<input checked="" type="checkbox"/>	En el transcurso de la documentación, ¿se adopta alguna medida para impedir la pérdida o el acceso indebido a la información que contienen los soportes o documentos, incluso los contenidos en anexos a un soporte electrónico, fuera de los locales del responsable del fichero o tratamiento caso autorizada por el responsable del fichero o se encuentra debidamente autorizada en el documento de seguridad?	No aplica	⊗
<input checked="" type="checkbox"/>	Los soportes que contienen datos de carácter personal del sistema de información, ¿permiten identificar el tipo de información que contienen? En el momento que se requiere sea afirmativa, indicar cuál es el mecanismo de identificación utilizado (mediante etiquetas, otros) adjuntando, al tiempo que la evidencia, el documento en el que se encuentra reflejada o incorporada esta información.	No	⊗
<input checked="" type="checkbox"/>	Los permisos que realizan recepción de soportes informáticos con datos de carácter personal, están debidamente autorizados en el documento de seguridad?	No aplica	⊗
<input checked="" type="checkbox"/>	¿Se adopta alguna medida para impedir la recuperación indebida de la información que contienen los documentos o soportes que contengan datos de carácter personal, cuando estos vayan a desasignarse? En el caso de responder afirmativamente, indicar cuál es la medida que impide la recuperación implementada (comparación con series de eliminación de los soportes, en papel o magnéticos, formato de datos, formato físico de los datos, utilización de aparatos de destrucción física de los soportes, procedimientos de recogida de soportes desasignados o su destrucción (carcinizada, otros) adjuntando, al tiempo que la evidencia, el documento en el que se encuentra reflejada o incorporada esta información.	No aplica	⊗
<input checked="" type="checkbox"/>	¿Se hace un registro de entrada de soportes informáticos?	No aplica	⊗
<input checked="" type="checkbox"/>	¿Se hace un registro de salida de soportes informáticos?	No aplica	⊗
<input checked="" type="checkbox"/>	¿Se han definido los procedimientos de realización de copias de respaldo (backups)?	No aplica	⊗
<input checked="" type="checkbox"/>	¿Se han definido los procedimientos de recuperación de los datos (recovery)?	No	⊗
<input checked="" type="checkbox"/>	Los procedimientos de respaldo y recuperación de datos definidos, ¿garantizan la reconstrucción del estado en que se encuentran los datos del sistema de información en el momento de producirse su pérdida o destrucción?	No aplica	⊗

Delegar | Aplicar a otros Sist.Inf. | Guardar | Confirmar | Recargar

Backups:

y por último, una vez cerrada la auditoría y generado el correspondiente informe, se pueden gestionar las recomendaciones obtenidas.

## 1 Entorno de Ejecución de la Aplicación

La aplicación está desarrollada en Java y se ejecuta sobre un servidor Jboss en Windows 2008 Server, siendo el gestor de Bases de Datos SQL Server 2005.