CAPÍTULO 4
AUDITORÍA SOBRE LA PROTECCIÓN DE DATOS: FASE 1ª

1. INTRODUCCIÓN

Al amparo del derecho a la privacidad recogido en el artículo 18 de la Constitución Española, surge la Ley Orgánica de Protección de Datos de carácter personal (LOPD-15/1999) que sustituye y amplia a la antigua LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos).

La LOPD genera además una relación de medidas técnicas concretas, que se recogen en el reglamento de desarrollo de la LOPD, de obligado cumplimiento para las empresas, este reglamento obliga a dichas empresas a establecer unas medidas organizativas y técnicas concretas encaminadas a garantizar el correcto tratamiento de los datos.

En el artículo 96 del reglamento, hace mención a la auditoría, y especifica lo siguiente:

> 1. *A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de la Ley.*
>
> *Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficiencia de las mismas. Esta auditoría inicia el cómputo de dos años señalados en el párrafo anterior.*

2. *El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias.*

   Deberá, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. *Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevara las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedaran a disposición de la Agencia de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas.*

2. OBJETIVO Y ALCANCE

Los objetivos son los siguientes:

- Comprobar la adecuación de las medidas, los procedimientos y controles de seguridad establecidos por el cliente, al Reglamento de Desarrollo e instrucciones vigentes en materia de seguridad de datos, y así disponer del documento de obligado mantenimiento en el artículo 88 de la RDLOPD.
- Comprobar la adecuación de las medidas, implantadas por el cliente, a las obligaciones formales descritas en la LOPD, para establecer los riesgos de infracción que pueden presentarse.

Alcance principal:

- La auditoría se realizará en el centro principal, siendo el mismo el reflejo de las prácticas establecidas en los demás centros de la organización. La documentación estudiada será limitada a los documentos genéricos utilizados en toda la organización.
- Como medida adicional, se realizarán visitas a otro centro para corroborar los aspectos más importantes, y cubrir aspectos específicos de ciertos departamentos. Redacción de cláusulas para formularios, circulares y contratos.

PROGRAMA DE AUDITORÍA (CRONOGRAMA)			
Tipo de auditoría:	Auditoria de la LOPD		
Equipo auditor	**Auditor Jefe**: D. Antonio Ruiz Escalante **Equipo auditor**: D. Antonio Ruiz Escalante, María Palma Rodríguez		
Objetivo:	Comprobar si las medidas y procedimientos utilizados en la implantación de la LOPD se adecuan a lo establecido en la Ley.		
Alcance:	La auditoría se realizara en el centro principal, en caso de que existan otros centros secundarios, se podrían realizar visitas, como medida adicional.		
Normativa:	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos y R.D. 1720/2007, 21 de Diciembre.		
Preparado por:	D. Antonio Ruiz Escalante.		
Fecha	**Hora**	**Área/ Actividades auditadas**	**Responsables**
14/02/06	09.00 am	Reunión de apertura o inicial	D. Fernando Ruiz Salas. D. Emilio Gómez Gutiérrez.
		Reunión de cierre	

3. OBLIGACIONES PREVIAS ANTES DE AUDITAR

INSCRIPCIÓN DE LOS FICHEROS EN LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

Toda persona o entidad que posea ficheros con datos personales está obligada a inscribir en el Registro General Protección de Datos, la estructura de los ficheros de que disponga. (Artículo 26.1 LOPD).

En concreto, de conformidad con el artículo 20 LOPD, la creación, modificación o supresión de los ficheros de las administraciones públicas solo podrán hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario correspondiente.

Información al interesado, como titular de sus datos, de la existencia del fichero y su finalidad.

Este deber se refiere al derecho que tiene el sujeto, cuyos datos personales han sido recabados de ser informado "de modo expreso, preciso e inequívoco" de conformidad con los artículos 5 y siguientes de la LOPD.

ADOPTAR LAS MEDIDAS DE ÍNDOLE TÉCNICA Y ORGANIZATIVAS NECESARIAS QUE GARANTIZAN LA SEGURIDAD DE DATOS

Además de las obligaciones anteriormente relacionadas y exigidas en la LOPD, el R.D. obliga a adoptar unas medidas de seguridad con el fin de proteger los datos de carácter personal contenidos en los ficheros, tanto automatizados (informáticos) como no automatizados (papel o manual). El R.D. distingue tres niveles de seguridad (básico, medio y alto), en función de la naturaleza de la información de carácter personal tratada.

CREACIÓN DE UN DOCUMENTO DE SEGURIDAD

De obligado cumplimiento para el personal con acceso a los datos de carácter personal y a los sistemas de información.

INFORMACIÓN AL PERSONAL DE LAS NORMAS DE SEGURIDAD Y CONSECUENCIAS DE SU INCUMPLIMIENTO

Es obligación del Responsable del Fichero o Tratamiento, informar, definir y documentar las funciones y obligaciones de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información en cumplimiento de lo establecido en el R.D.

OBLIGATORIEDAD DE QUE CONSTE POR ESCRITO EL ENCARGO DEL TRATAMIENTO DE LOS DATOS POR CUENTA DE UN TERCERO, Y QUE SE ACUERDEN LAS MEDIDAS DE SEGURIDAD QUE HA DE CUMPLIR

Todo acceso, por cuenta de terceros, a los datos personales contenidos en los ficheros titularidad del Responsable del Fichero o Tratamiento, que resulte necesario para la prestación de un servicio, deberá ser regulado mediante un contrato, de conformidad con el artículo 12 de la LOPD.

PROHIBICIÓN DE COMUNICAR O CEDER LOS DATOS PERSONALES A UN TERCERO SIN CONSENTIMIENTO PREVIO DEL INTERESADO

Una de las principales obligaciones, consiste en obtener el consentimiento, en los supuestos establecidos por la LOPD de aquellos, de quienes se recaban los datos de carácter personal. No obstante, la propia LOPD contempla una serie de excepciones a la citada obligación, tanto para el tratamiento (Art. 6.2) como para la cesión (Art. 11.2).

4. Metodología de trabajo

La primera actividad a realizar es una reunión inicial, en la que se presentarán todas aquellas cuestiones relativas al Plan de atrabajo, calendario, planificación, participantes, interlocutores, reuniones, etc.

Antes del comienzo de la auditoría, es conveniente que el auditor se reúna con la dirección de la entidad que va a auditar, con la finalidad de tratar los puntos siguientes:

- Presentación del equipo auditor.
- Exposición de los objetivos y programa de realización de la auditoría.
- Confirmar los canales de comunicación entre auditor y empresa auditada, además de proporcionar información sobre las fechas propuestas para las visitas, o inspección visual, así como la estimación de los encuentros entre ambas partes.
- Indicación de la metodología y procedimiento a utilizar y confirmación de la disponibilidad de los medios necesarios para el desarrollo correcto de la auditoría.

- Concreción de la fecha de la reunión final y de cualquier otra reunión intermedia entre el equipo auditor y la dirección auditada.
- Proporcionar al auditado la oportunidad de realizar preguntas, para la clarificación de las cuestiones confusas del programa de la auditoría.

4.1. PLANIFICACIÓN DE LA AUDITORÍA

El auditor para la ejecución de la auditoría necesitará una herramienta que le permita examinar de manera ordenada todos aquellos elementos que hubiera previsto abordar.

La herramienta más utilizada en el ámbito de las auditorías son las **listas-guias** o **chec-list**. Son documentos en los que se enumeran una serie de puntos que irán tratándose conforme avance la auditoría.

A la hora de planificar una auditoría tendrían que tenerse en cuenta los siguientes puntos:

- Los objetivos y alcance de la auditoría.
- El criterio a ser usado para la realización de la auditoría.
- La identificación de las unidades organizadoras y funcionales auditadas.
- La identificación de las funciones o individuos dentro de la organización del auditado que tengan responsabilidades relativas a la protección de datos.
- Identificación de los documentos de referencia.
- El tiempo y duración esperada para las entrevistas e inspecciones.
- Las fechas y lugares donde se va a realizar la auditoría.
- El cronograma de reuniones que se van a tener con la gerencia del auditado.
- Requerimientos confidenciales.
- El contenido, formato y estructura del informe.

4.2. SOLICITUD Y ANÁLISIS DE LA DOCUMENTACIÓN

Para poder llevar a cabo la auditoría de protección de datos, el auditor debe solicitar la información y documentación necesaria para el conocimiento orientati-

vo de las circunstancias generales y particulares de la entidad que le permitan valorar si dicha empresa se adecua a la protección de datos, además de una comprensión de la organización en su conjunto.

El auditor deberá preparar una lista de aquellos documentos que serán solicitados, dado que no es recomendable presentarse en la organización a auditar y pedir documentación sin una previsión, o ir solicitándola periódicamente según el momento de la auditoría.

Los documentos que pueden solicitarse en esta fase, son los siguientes:

- Documentos generales de la entidad:
  - Datos básicos: nombre, dirección, NIF, numero de trabajadores, centros de trabajo, etc.
  - Descripción de la actividad.
  - Organigrama.
  - Manual del empleado.
- Documentos específicos de la protección:
  - El documento de seguridad.
  - Justificantes documentales de la implantación de dicho documento.
  - Contratos de Encargo(los contratos realizados con los encargados de tratamiento).
  - Certificados de inscripción de los ficheros emitidos por la Agencia Española de Protección de Datos.
  - Contratos de migración de datos si existieran transferencias internacionales de datos.
  - Cláusulas de confidencialidad y deber de secreto para aquellas prestaciones de servicio sin acceso a datos.

4.3. ELABORACIÓN DE UN PROGRAMA DE AUDITORÍA

Una vez realizada la planificación es necesario elaborar un programa de auditoría, en su preparación se deben tener presentes los recursos humanos que se van a utilizar y el tiempo de que se dispone.

Este programa debe confeccionarse antes del inicio del trabajo, de forma que se conozca desde el principio dónde y cuándo se deben realizar las diferentes

actividades que constituyen las fases de ejecución de la auditoría, y las personas que participan en ella. Son las siguientes:

- Programa de actuación.
- Interlocutores que participan en cada una de las actividades.

PROGRAMA DE AUDITORÍA				
Cliente D. Juan García Díaz				
Orden de trabajo				
Fecha de inicio	**Fecha final**	**Tarea**	**Auditor**	**Supervisor**
14/02/09	20/02/09	Auditoría de la LOPD	Antonio Ruiz Escalante	María Palma Rodríguez

AGENDA DEL AUDITOR									
Cliente : Juan García Díaz									
Orden de trabajo: Examen de la documentación, entrevista con el personal, inspección visual.									
Auditor: D. Antonio Ruiz Escalante									
Fecha :14/02/09									
Personal a entrevistar: responsable de los ficheros y encargado de tratamiento de datos de las áreas auditadas.									
Areas auditadas: niveles de seguridad, funciones y obligaciones del personal registro de incidencia, control de acceso a datos de carácter personal.									
Desglose Horario									
9-10	**10-11**	**11-12**	**12-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**7-8**

5. 1ª Fase de la auditoría de la Ley de Protección de Datos

1ª fase: identificación de los datos personales

En ella se obtiene el mayor volumen de información posible, necesaria para poder desarrollar y elaborar la Política de Seguridad a seguir, así como para desarrollar el resto de fases de la auditoría.

En esta fase el equipo auditor se desplazará, en caso de ser necesario, a la empresa o centro de trabajo correspondiente para poder llevarla a cabo.

En esta fase se analizará lo siguiente:

- Identificación de los datos y ficheros que deben ser protegidos.
- Identificación de Usuarios con acceso a los ficheros.
- Identificación de medios, sistemas a utilizar para la protección de dichos ficheros.
- Clasificación de ficheros: nivel bajo, medio o alto.

En esta fase se tendrá en cuenta también el cumplimiento de una serie de obligaciones que impone la LOPD, que son las siguientes:

- **Calidad de los datos**

  Los datos de carácter personal solo se podrán recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado y serán cancelados cuando hayan dejado de ser necesarios o pertinentes (Art. 4 LOPD).

- **Deber de Secreto**

  El Responsable del Fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secre-

to profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero (Art. 10 LOPD).

- **Información en la recogida de datos**

  Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, estas advertencias (Art. 5 LOPD).

- **Consentimiento del afectado**

  El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa, sea una AA.PP, sean necesarios para un contrato o figuren en fuentes accesibles al público. Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Estos aspectos anteriores y los datos sobre origen racial, salud o vida sexual solo pueden ser recogidos, tratados o cedidos, con el consentimiento expreso y por escrito del afectado. Sin embargo, estos tipos de datos sí podrán tratarse, cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario o equivalente, sujeto al secreto profesional (Art. 7 LOPD).

  Sin perjuicio de lo que se dispone en el artículo 11 de la LOPD respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes, podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad (Art. 8 LOPD).

CLAUSULA INFORMATIVA PARA EL TRATAMIENTO DE LOS DATOS PERSONALES DE LOS TRABAJADORES DE ACUERDO CON LO ESTABLECIDO EN LA LEY ORGANICA 15/1999 DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (LOPD)

\EMPRESA\
\DIRECCION\
\COD. POSTAL\ \POBLACION\

\TRABAJADOR\
\DNI TRAB\
\COD. POSTAL\ \PROVINCIA\

"\EMPRESA\" comunica a Don / Doña **"\TRABAJADOR\"** que sus datos personales recogidos en el contrato de trabajo suscrito con fecha "**\FECHA ALTA**" pasarán a formar parte de un fichero automatizado titularidad de **"\EMPRESA\"** y serán tratados por la Empresa, de acuerdo con la legislación vigente en materia de protección de datos personales, con la finalidad de mantenimiento de la relación laboral.

Los datos personales podrán ser comunicados a terceros sin el consentimiento del titular de los mismos siempre que esta comunicación responda a una necesidad para el desarrollo, cumplimiento y control de la relación laboral y se limita a esta finalidad, tal y como se establece el art. 11.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Para ejercitar los derechos de acceso, impugnación, rectificación, cancelación u oposición de sus datos, deberán dirigirse a **"\EMPRESA\"** y cumplimentar los formularios dispuestos al efecto.

FIRMA DEL TRABAJADOR

Fdo: **\TRABAJADOR**

ALMERIA, DD DE MM DE AAAA

- **Comunicación o cesión de datos**

  Los datos de carácter personal objeto del tratamiento solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento del interesado. Sin embargo este consentimiento no será preciso:

  – Cuando la cesión esté autorizada en una Ley.
  – Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica (cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros).
  – Cuando los datos procedan de fuentes accesibles al público.
  – Cuando la cesión sea de datos relativos a la salud y sea necesaria para solucionar una urgencia (que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica).
  – Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (Art. 11 LOPD).

- **Tratamiento por cuenta de terceros**

  Deberá estar regulado en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del Tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

  Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al Responsable del Fichero, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento. En el caso de que el Encargado del Tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considera-

do, también, Responsable del Tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

- **Inscripción de los ficheros**

  En el Registro General de la Agencia Española de Protección de Datos (RGPD), con previa publicación en Boletín Oficial de una Disposición General con la declaración de los ficheros (Artículo 20 LOPD).

- **Tutela del derecho de los afectados de acceso, rectificación y cancelación**

  Estableciendo el procedimiento interno apropiado.

- **Redacción e implantación del documento de seguridad**

  Que incluya toda la normativa de seguridad de índole técnica y organizativa necesaria para garantizar la seguridad de los datos objeto de tratamiento. Será de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información (Art. 9 LOPD y R.D. 1720/2007).

- **Auditoría**

  Cada dos años del cumplimiento de la legislación y de los procedimientos de seguridad (R.D. 1720/2007).

1. ¿En qué consiste el deber de secreto, como cumplimiento de una de las obligaciones de la LOPD?

2. ¿Cuál es la metodología de trabajo de la auditoría?

3. ¿Qué puntos deben tenerse en cuenta a la hora de realizar una auditoría?

4. ¿Qué debemos analizar en al 1ª fase de una auditoría?

5. ¿A partir de qué nivel es obligatorio realizar una auditoría?

EJERCICIOS DE REPASO Y AUTOEVALUACIÓN