Departamento de Informática

PROYECTO FIN DE CARRERA

PROTOTIPO DE HERRAMIENTA PARA LA AUDITORÍA DE MEDIDAS DE SEGURIDAD REQUERIDAS EN LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Autor: Silvia León Márquez

Tutor: Miguel Ángel Ramos González

Leganés, junio de 2015

Título: PROTOTIPO DE HERRAMIENTA PARA LA AUDITORÍA DE MEDIDAS DE SEGURIDAD REQUERIDAS EN LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Autor: Silvia León Márquez

Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 23 de Junio de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Agradezco a mi familia, y en especial a mis padres su apoyo constante e incondicional en toda mi vida.

Agradecer también a mi tutor, Miguel Ángel por su esfuerzo y dedicación, así como su paciencia y su motivación para poder llevar a cabo el desarrollo de este Proyecto.

Resumen

El presente Proyecto final tiene como título: “PROTOTIPO DE HERRAMIENTA PARA LA AUDITORÍA DE MEDIDAS DE SEGURIDAD REQUERIDAS EN LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL”.

El objetivo de este Proyecto es realizar un prototipo en Microsoft Excel para llevar a cabo la revisión y/o auditoría de las medidas de seguridad requeridas en la normativa de protección de datos, concretamente en el Reglamento de Desarrollo de la Ley Orgánica de protección de datos RLOPD Real Decreto 1720/2007.

Se ha realizado un análisis de la normativa de protección de datos, habiéndose analizado la normativa europea existente y la normativa española.

Este proyecto se ha centrado en el análisis del Título VIII del Reglamento de Desarrollo de la LOPD, donde se describen las medidas de seguridad que deberán contemplar los ficheros automatizados y no automatizados.

De esta forma, se han detallado la relación de pruebas específicas y aspectos a tener en cuenta en la normativa de protección de datos. Este programa de trabajo ha sido diseñado en un prototipo en Microsoft Excel por su facilidad de desarrollo, mantenimiento, uso y actualización.

Adicionalmente, se ha procedido a realizar un análisis de las nuevas tecnologías que han proliferado en los últimos años: etiquetas de radio-frecuencia (RFID), Big Data, Cloud Computing, Internet de las cosas, y su impacto en la privacidad y protección de datos.

Palabras clave: Protección de Datos, Privacidad, LOPD, RLOPD, Dato de carácter personal, Medidas de seguridad en sistemas automatizados, Medidas de seguridad en sistemas no automatizados.

Abstract

The present final career Project has as tittle “PROTOTYPE TOOL FOR AUDITING SECURITY MEASURES REQUIRED IN DATA PROTECTION LAW”.

The main objective of this Project is to design and develop a Microsoft Excel prototype that allows reviewing or auditing the security measures required in data protection regulation in Royal Decree 1720/2007.

An analysis of the data protection regulation has been realized, including European and Spanish regulation.

We have focused the report in the Title VIII of the Royal Decree 1720/2007: “Regarding security measures in the processing of personal data”, applicable to automated and non-automated files.

In this way, a workprogam has been detailed containing the different checks, tests and different aspects to be considered necessary to accomplish with the data protection regulation. This workprogram has been designed in Microsoft Excel because it is easy to develop, maintain, use and upgrade.

In addition, it has been realized and analysis of the New Technologies have became in last years: radio frequency identification, Big Data, Cloud Computing, Internet of the Things,.. and their impact on privacy and data protection.

Keywords: Data protection, Privacy, LOPD, RLOPD, personal data, Security measures applicable to automated files, Security measures applicable to non automated files.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción y objetivos

1.1 Introducción

Este primer capítulo contendrá aspectos generales y los objetivos de este Proyecto de Final de Carrera.

A lo largo de este capítulo se describirán por tanto los objetivos de este proyecto, las fases en las que se ha llevado a cabo así como los medios necesarios para la consecución del mismo.

Por último, se describirá un breve resumen de cada uno de los apartados de la memoria con una descripción de los aspectos fundamentales de cada uno de los apartados.

1.2 Principales objetivos

El objetivo fundamental de este Proyecto es realizar un programa de trabajo desarrollado en un prototipo en Microsoft Excel que permita llevar a cabo la revisión y/o auditoría de las medidas de seguridad requeridas en el Título VIII del Reglamento de Desarrollo de la Ley Orgánica de protección de datos.

De esta forma, se pretende llevar a cabo un análisis de la normativa de protección de datos en la actualidad, a partir de la norma existente, nos centraremos en cómo llevar a cabo una auditoría o revisión del cumplimiento de las medidas de seguridad exigidas por la normativa. En base a ese objetivo principal, se proponen los siguientes objetivos parciales:

- **Análisis normativa existente de protección de datos**:
  - Marco Europeo.
  - Marco español.
  - Resto normativas o herramientas jurisdiccionales que sea necesario tener en consideración.
  - Autoridades de control de protección de datos.

- **Análisis marco general Auditoría:**
  - Aspectos generales de Auditoría.
  - Tipos de Auditoría.
  - Aspectos requeridos en una Auditoría de la normativa de protección de datos.
  - Elaboración de programa de trabajo de auditoría, identificando pruebas a realizar, cómo llevar a cabo la evaluación de las mismas y resultados.

- **Análisis detallado de las medidas de Seguridad requeridas por la normativa de protección de datos**
  - Análisis de aspectos que se recogen en la normativa.
  - Identificación de aspectos a tener en cuenta en cumplimiento de la normativa.

- **Evolución normativa y novedades:**
  - Análisis evolución normativa de protección de datos.
  - Búsqueda de información sobre novedades normativas en Informes y/o análisis jurídicos.
  - Novedades tecnológicas y protección de datos.

- **Desarrollo prototipo:**
  - Establecimiento del programa de trabajo en Microsoft Excel.
    El prototipo ha sido desarrollado en Microsoft Excel por su sencillez y por el hecho de que puede ser utilizado en prácticamente cualquier ordenador personal sin requerir necesidades técnicas especiales o software específico.

  - Desarrollo conexión con Microsoft Word para la obtención del Informe de Auditoría.

Es importante señalar que se han incluido referencias a los textos normativos de forma que quede más claro qué es lo que dice exactamente la normativa y a partir de ahí, las interpretaciones y/o aclaraciones que he analizado tras la búsqueda de información en la Bibliografía incluida en el último apartado. Se han incluido estas referencias en otro formato de texto para que se identifique fácilmente.

1.3 Fases del desarrollo

El desarrollo del proyecto se ha dividido en un conjunto de fases y subfases que se desglosan a continuación:

- **Fase I: Determinación del alcance y objetivos**
  En esta fase se ha procedido a realizar los aspectos iniciales del proyecto, determinar su alcance y los objetivos a conseguir. Se compone de las siguientes subfases:

  I. Identificación objetivos y alcance
  En esta subfase se describen los objetivos del proyecto y se delimita el alcance del mismo; se analiza también los aspectos que se incluirá en relación a nuevas normativas

  II. Propuesta de contenidos
  En esta subfase se describen los contenidos que contendrá el proyecto y la definición de la estructura de la memoria que se llevará a cabo.

  III. Análisis información encuestas e importancia
  En esta subfase se ha analizado la importancia que tiene considerada la protección de datos y la privacidad en la sociedad actual, para ello se ha procedido a recabar información procedentes de encuestas llevadas a cabo por el Centro de Investigaciones Sociológicas.

- **Fase II: Análisis normativa de protección de datos**

  I. Análisis normativa europea
  En esta subfase se ha analizado el marco europeo de protección de datos.

  II. Análisis normativa española
  En esta subfase se ha analizado el marco europeo español relativo a la protección de datos.

  Para ello, se ha realizado un análisis desde la Constitución Española la normativa específica de protección de datos.

  III. Análisis información Autoridades de Control
  En esta subfase se ha analizado la autoridad de Control española así como las diferentes autoridades de control autonómicas existentes en la normativa de protección datos.

  Adicionalmente, se ha procedido a llevar a cabo un estudio sobre las funciones de cada una de ellas y las diferencias entre sí, de igual forma se ha procedido a llevar a cabo un análisis de las memorias anuales de la AEPD para mostrar los valores relativos a la actividad de la Agencia.

- **Fase III: Análisis medidas de seguridad Título VIII**

  I. Aspectos generales Auditoría
  En esta subfase se ha analizado los aspectos básicos de Auditoría, las distintas clases de auditoría así como las fases en las que se desarrolla la misma.

  II. Medidas de Seguridad sistemas automatizados: análisis y definición de pruebas
  En esta subfase se ha analizado en detalle las medidas de seguridad que se recogen en el Título VIII referido a sistemas automatizados para cada uno de los niveles: básico, medio y alto, elaborando un programa de trabajo con cada una de las pruebas y aspectos a tener en cuenta en cumplimiento de la normativa.

  III. Medidas de Seguridad sistemas no automatizados: análisis y definición de pruebas
  En esta subfase se ha analizado en detalle las medidas de seguridad que se recogen en el Título VIII referido a sistemas no automatizados para cada uno de los niveles: básico, medio y alto, elaborando un programa de trabajo con cada una de las pruebas y aspectos a tener en cuenta en cumplimiento de la normativa.

- **Fase IV: Diseño prototipo**

  I. Análisis y definición de requisitos
  En esta subfase se ha llevado a cabo un análisis y definición de los requisitos a tener en cuenta para la elaboración del programa de trabajo.

  II. Diseño detallado
  En esta subfase se ha llevado a cabo el diseño del programa de trabajo en el prototipo.

  III. Conexión Word y definición de Formato Informe Auditoría
  En esta subfase se ha llevado a cabo la identificación de información necesaria para el establecimiento del informe de Auditoría y el desarrollo con las herramientas Visual Basic facilitadas por Microsoft Excel para exportar esta información a Microsoft Word.

  IV. Pruebas de funcionamiento
  En esta subfase se ha llevado a cabo pruebas de funcionamiento para verificar si el prototipo funcionaba correctamente y si el volcado de información es el adecuado en cumplimiento de los objetivos propuestos.

  V. Depuración errores de funcionamiento
  En esta subfase se han depurado incidencias y/o errores detectados, proponiéndose mejoras en el prototipo diseñado.

- **Fase V: Evolución normativa**

  I. **Evolución normativa y posturas doctrinales**
  En esta subfase se ha llevado a cabo un análisis de la evolución de la normativa de protección de datos desde la aprobación del RLOPD a la actualidad, identificando aquellos aspectos más significativos.

  De igual forma, se ha analizado las distintas posturales doctrinales de la autoridad de control, para ello, se ha seleccionado aquéllos más relevantes en relación a la auditoría de medidas de seguridad.

  II. **Nuevas tecnologías y nuevos retos**
  En esta subfase se ha llevado a cabo un análisis de las nuevas tecnologías existentes y la implicación así como los riesgos más significativos en cumplimiento de la normativa de protección de datos.

- **Fase VI: Memoria y documentación**

  I. **Memoria y documentación**
  Esta subfase se ha llevado durante el desarrollo de todo el proyecto y ha consistido en la documentación de la memoria del proyecto de cada una de las fases,

  II. **Revisión y verificación**
  En esta subfase se incluyen las tareas de revisión y verificación de la memoria final.

1.4 Medios empleados

Los medios empleados para la realización de este proyecto son:

- Software base Windows equipo informático.
- Software ofimático Office: Microsoft Word y Microsoft Excel.
- Visual Basic para Aplicaciones de Microsoft Office.
- Bibliografía.
- Recursos en Internet, en especial la información facilitada por la Agencia Española de Protección de Datos
- Asistencias a charlas y conferencias.

1.5 Esquema de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de cada capítulo.

A lo largo de todo el Documento se analizará la protección de datos desde diferentes ámbitos, dentro de los objetivos marcados en este proyecto se encuentran:

- **Introducción a la protección de datos**
  En este capítulo se describe brevemente los conceptos básicos de la protección de datos. Se presentará también un estudio acerca de la protección de datos en España.

- **Marco legislativo de la protección de Datos.**
  En este capítulo se detalla tanto el marco Europeo, donde se establecen normas y directivas comunitarias, así como el marco español, desde la Constitución Española hasta el Reglamento de Desarrollo de la LOPD.

  En este capítulo se incluye también una descripción Detallada del RLOPD, para cada uno de los Títulos que componen el RLOPD los aspectos más importantes y significativos, a excepción del Título VIII referido a las medidas de Seguridad, que será descrito en una sección específica.

- **Agencia Española de Protección de Datos**
  Se incluye un capítulo en relación a la Agencia Española de Protección de Datos, que es el órgano público español encargado de la vigilancia del cumplimiento de la protección de datos.

  Donde se analiza la información acerca de la actividad de la Agencia Española, cómo órgano público encargado de la vigilancia del cumplimiento de la protección de datos en España y las cifras relativas a inspecciones y sanciones a partir de la información de las Memorias Anuales de la Agencia Española de Protección de Datos.

- **Cumplimiento de las medidas de Seguridad del Título VIII del RLOPD**
  En este capítulo se analiza en detalle el Título VIII del Reglamento de Desarrollo de la LOPD, analizando en cada uno de los aspectos exigidos:

  - aspectos a tener en cuenta en la normativa, tanto organizativos como técnicos.
  - áreas que cómo auditor tendríamos que tener en cuenta en una revisión.
  - cómo debería revisarse la información, buenas prácticas o aspectos que un auditor debería considerar en la evaluación de la información que se esté analizando.

- **Evolución normativa en materia de protección de datos**
  En este capítulo se incluyen aspectos normativos en referencia a protección de datos desde la entrada en vigor del Reglamento de Desarrollo de la LOPD.

  De esta forma dentro de este capítulo se incluyen disposiciones, cambios en la normativa que han ido reformando el Reglamento y la Ley Orgánica de Protección de Datos; de igual forma se incluyen algunos aspectos de interpretación de temas de protección de datos que se han obtenido de la propia Agencia Española de Protección de Datos.

Capítulo 2

Introducción a la protección de datos de carácter personal

2.1 Significado de protección de datos de carácter personal

Como primer aspecto fundamental es necesario determinar qué se entiende en la normativa por dato de carácter personal, de esta forma se define como cualquier dato capaz de identificar por sí mismo a una persona física. En tal sentido, se entiende por dato personal cualquier información concerniente a personas físicas identificadas o identificables.

Dentro de éstos, por tanto se encuentran el nombre y apellidos, DNI, dirección, etc.

Adicionalmente existe un conjunto de datos que por sí solos no identificarían a una persona, es el caso de la edad, el sexo, etc. Los cuales por sí solos no permiten identificar a una persona y que sin embargo, agrupados con un dato identificativo se convierten en datos de carácter personal y por tanto, deben estar regulados por la normativa de protección de datos.

La protección de datos de carácter personal pretende garantizar al titular de los datos que los terceros, ya se trate del sector público o privado, utilizarán sus datos personales

con el respeto debido, de forma que aquél pueda tener un control sobre sus datos y en todo momento tenga conocimiento de:

- qué se va a hacer y quien trata sus datos
- para qué se recaban los datos
- cómo se tratan los datos
- para qué se utilizan
- a quién se ceden o comunican los datos
- eliminación de los datos cuando ya no sean necesarios

Es necesario indicar que, la protección de datos es un derecho fundamental, y como tal, ha de ser respetado por todos, desde el propio titular de los mismos.

Como se analizará más adelante, existe distintos niveles de clasificación en función de la tipología de datos de carácter personal; de esta forma deben establecerse aquellos que por su naturaleza son especialmente sensibles, dentro de estos podemos diferenciar:

- Datos especialmente protegidos: datos de carácter personal que revelen ideología, afiliación sindical, religión, creencias, origen racial y vida sexual.
- Datos relativos a salud del propio afectado o del entorno familiar.

2.2 La preocupación ciudadana por la protección de datos

2.2.1 Utilización de los datos en Internet

Últimamente en la sociedad actual existe una preocupación de sobre el uso y tratamiento de los datos en Internet, lo que hace necesario que los ciudadanos no sólo conozcan la normativa que les protege y los derechos que les reconoce sino, también, que su nivel de concienciación se adapte a los nuevos riesgos que afectan a su privacidad.

El Centro de Investigaciones Sociológicas (CIS) realizó en mayo de 2013, un estudio, donde se incluyen aspectos en relación a la concienciación de los ciudadanos en relación a la seguridad de la información y la protección de los datos personales.

En este estudio, se tratan los siguientes aspectos:

- Preocupación sobre distintos temas: avance de la ciencia y la tecnología, la protección de los datos personales y el desarrollo de la comunicación a través de Internet.
- Seguridad en la protección de datos personales de determinadas actividades asociadas a pagos, compras, etc.
- Recepción de publicidad y cancelación de datos.

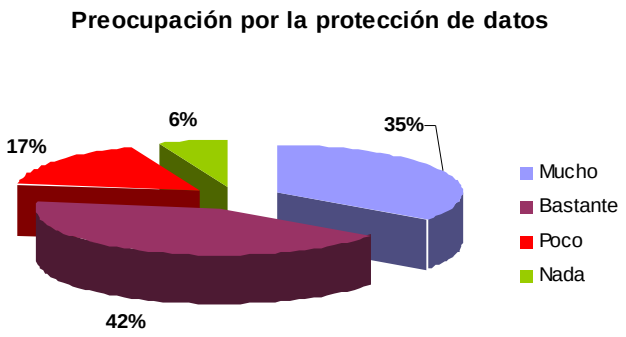


Figura 1: Encuesta CIS Barómetro Mayo 2013 Preocupación ciudadana

Los datos del barómetro son claros al reflejar las siguientes conclusiones:

- Que el porcentaje de ciudadanos preocupados por la protección de datos y el uso de la información personal (tipificado como "mucho" y "bastante") continúa creciendo y alcanza al 76,3% de los encuestados.

- Que el 50% y el 66% de los ciudadanos valoran de manera alta o muy alta la seguridad de sus datos que tratan los bancos y Administraciones Públicas respectivamente.

- Que el 46,1% se considera muy informado/bastante informado acerca de los riesgos que puede conllevar el proporcionar datos personales.

- Más del 90% de los ciudadanos que los menores de edad deberían tener controles en el acceso a Internet.

- Que el 70% de los encuestados ha recibido publicidad a través de correo electrónico de una entidad a la que no se han facilitado los datos.

A la vista de todos estos porcentajes se puede llegar a la conclusión que los ciudadanos, poco a poco se han ido sensibilizando sobre la protección de sus datos personales debido a la preocupación que tienen en proteger su esfera personal e íntima.

2.2.2 Protección de datos y seguridad ciudadana

La creciente preocupación que existe en proteger la esfera íntima y personal de los ciudadanos entra en conflicto, en muchas ocasiones, con el concepto de seguridad.

Con respecto a la colisión de estos dos conceptos, el Centro de Investigaciones Sociológicas llevó a cabo en el barómetro de Septiembre 2009 determinados aspectos en relación a Seguridad ciudadana.

2.2 LA PREOCUPACIÓN CIUDADANA POR LA PROTECCIÓN DE DATOS

En este estudio, se tratan los siguientes aspectos:

- Posicionamiento ante la existencia de cámaras de seguridad o videovigilancia. Razones para estar a favor o en contra de su existencia.
- Valoración de la existencia de cámaras de seguridad o videovigilancia en bancos, comercio, comunidades de vecinos, lugares de trabajo, calles, hospitales, transporte público, y bares.
- Conocimiento de la necesidad de autorización y señalización de las cámaras de seguridad.

A la vista de los resultados, se refleja un empate entre ambos aspectos, ya que la mayoría de los encuestados se sitúan en una posición intermedia si tienen que elegir entre libertad y seguridad.

Así, el 68,7% de ellos se muestra a favor de la colocación de sistemas videovigilancia porque:

- proporciona más seguridad (66,4%)
- permite la identificación de los delincuentes (18,0%)
- y evita delitos (15,2%)

En este sentido, los lugares en los que más partidarios se muestran en la instalación de los mismos se centra en: bancos (95.5%), en comercios (88.3%) y en guarderías y colegios (77.2%).

Sin embargo, el 10% se posiciona en contra de la instalación de cámaras al considerar que con su instalación se produce una pérdida de intimidad (79,4%).

Los lugares donde son menos partidarios los ciudadanos a la instalación de cámaras son: los locales de trabajo (36,7%), y bares y restaurantes (36%).

Por lo tanto, y a vista de los resultados obtenidos en la encuesta realizada por el CIS, el concepto clave a la hora de limitar la privacidad en aras de reforzar la seguridad es la proporcionalidad.

La percepción positiva sobre los sistemas de videovigilancia en los distintos entornos y ámbitos de la vida diaria deberá ir siempre acompañada de la exigencia de ciertas garantías encaminadas a proteger la privacidad, por lo que se hace necesario encontrar un equilibrio entre ambas.

CAPÍTULO 2: INTRODUCCIÓN A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Capítulo 3

Marco legislativo de la protección de datos

3.1 Marco europeo

3.1.1 Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos es un documento declarativo adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París, que recoge los derechos humanos considerados básicos.

La unión de esta declaración y los Pactos Internacionales de Derechos Humanos y sus Protocolos comprende lo que se ha denominado la Carta Internacional de Derechos Humanos.

Mientras que la Declaración constituye, generalmente, un documento orientativo, los Pactos son tratados internacionales que obligan a los Estados firmantes a cumplirlos.

3.1.2 Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales

La Convención Europea de Derechos Humanos fue adoptada por el Consejo de Europa en 1950 y entró en vigor en 1953. El nombre oficial de la Convención es Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Tiene por objeto proteger los derechos humanos y las libertades fundamentales, y permite un control judicial del respeto de dichos derechos individuales. Hace referencia a la Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948.

En su artículo 8 relativo al Derecho al respecto de la vida privada y familiar:

[1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber ingerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta ingerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.]

3.1.3 Convenio 108 del Consejo de Europa

El Convenio 108/1981, del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, elaborado en Estrasburgo el 28 de enero de 1981 y ratificado en España mediante instrumento de 31 de enero de 1984, tiene por objeto garantizar en el territorio de cada parte, a cualquier persona física, el derecho a la vida privada, con respecto al tratamiento de los datos de carácter personal.

En su artículo 1 establece que tiene por objeto:

[El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos.]

La finalidad del Convenio es garantizar a cualquier persona el respeto de sus derechos y libertades fundamentales, especialmente su intimidad, mediante la ordenación de la utilización de la Informática en la gestión de los datos personales, fijándose unos límites para que los datos de carácter personal puedan ser almacenados, registrados y tratados, así como el establecimiento de garantías jurídicas de defensa frente a actividades contrarias al Convenio.

Dentro del Convenio se establecían una serie de principios y derechos que han sido recogidos en el ordenamiento español en lo que sería posteriormente la LORTAD y después la LOPD.

a. Principio de lealtad y legalidad: Los datos procesados se obtendrán y tratarán de forma legal y legítima.
b. Principio de proporcionalidad: los datos serán registrados para las finalidades determinadas legítimas y no se utilizarán de forma incompatible a dichas finalidades. Adicionalmente los datos serán adecuados, pertinentes y no excesivos en relación a dichas finalidades.
c. Principio de exactitud: los datos serán exactos y se mantendrán actualizados.

Estos principios se establecen en su artículo 5, referido a la Calidad de datos:

> *[Los datos de carácter personal que sean objeto de un tratamiento automatizado:*
> *a) Se obtendrán y tratarán leal y legítimamente;*
> *b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;*
> *c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;*
> *d) serán exactos y si fuera necesario puestos al día;*
> *e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.]*

d. Principio de Seguridad de los datos. En su artículo 7, establece:

> *[Se tomarán medidas de seguridad apropiadas para la protección de los datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.*

e. Protección de datos sensibles: se refuerza la protección de datos que con informaciones referentes al origen racial, opiniones políticas, religiosas, datos relativos a salud, vida sexual o antecedentes penales.

   Artículo 6, referente a categorías particulares de datos:

> *[Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.]*

f. Principio de acceso a los ficheros automatizados

   En relación a las Garantías complementarias para la persona concernida, en su artículo 8, se establece que:

> *[Cualquier persona deberá poder:*
> *a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;*
> *b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;*
> *c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;*

> *d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.]*

El Convenio establece también una serie de excepciones y restricciones a los derechos:

1. Que se establezcan por ley excepciones a la garantía de los derechos de los ciudadanos cuando sean medidas necesarias y justificadas por los siguientes motivos:
    a. La defensa de los intereses del Estado.
    b. Mayor protección de la persona afectada o de los derechos y libertades de terceros.

    Establecido en su artículo 9.2:

    > *[Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:*
    >
    > *a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;*
    >
    > *b) para la protección de la persona concernida y de los derechos y libertades de otras personas.]*

2. Que la ley no pueda prever restricciones al ejercicio del derecho al conocimiento, rectificación y cancelación de los propios datos en el caso de ficheros automatizados de datos de carácter personal que se utilizan con finalidades estadísticas o de investigación científica cuando no existan, de forma manifiesta, riesgo de atentado a la vida privada de las personas afectadas.

3.1.4 Carta de los Derechos Fundamentales de la Unión Europea

La Carta de los Derechos Fundamentales de la unión Europea fue proclamada solemnemente en el Consejo Europeo de Niza los días 7 a 9 de diciembre de 2000.

Dentro de su Capítulo II, denominado “Libertades”, se incluye el derecho a la protección de datos de carácter personal, artículo 8:

> *[1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.*
>
> *2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.*
>
> *3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.]*

3.1.5 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre

La Directiva 95/46/CE constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea.

Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

La Directiva se aplica a los datos tratados por medios automatizados, así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él.

La Directiva deja fuera del ámbito de aplicación determinados tratamientos de datos:

- efectuado por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas.
- aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

- Calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.

- Legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:
    - la ejecución de un contrato en el que el interesado sea parte.
    - el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento.
    - proteger el interés vital del interesado.
    - el cumplimiento de una misión de interés público.
    - la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

- Las categorías especiales de tratamiento: debe prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las

convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

- Información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.

- Derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:
    - Confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos.
    - Rectificación, supresión o bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.

- Excepciones y limitaciones: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.

- Derecho del interesado a oponerse al tratamiento: el interesado tendrá derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento.
  También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

- Confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento.
  El responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

- Notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento.
  La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación.

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados.

Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado, por el contrario, no se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo excepciones concretas que se establecen en la Directiva.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.

Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión.

3.1.6 Reglamento (CE) nº 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000

Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a libre circulación de estos datos.

En concreto, respecto a los datos, estos datos deben ser:

- Tratados de manera leal y lícita.
- Recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines.
- Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.
- Exactos y, cuando sea necesario, actualizados (se tomarán todas las medidas razonables para la supresión o rectificación de los datos inexactos o incompletos en relación con los fines para los que fueron recogidos o para los que fueron tratados posteriormente).
- Conservados en una forma que permita la identificación de los interesados durante un periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten posteriormente.

En el Reglamento se prevé, asimismo, el establecimiento de una autoridad europea independiente de control responsable de velar por la debida ejecución de las disposiciones relativas a la protección de datos por las instituciones y los organismos de la UE, denominada "Supervisor Europeo de Protección de Datos".

Se indica que esta figura será comparable a las autoridades del mismo tipo establecidas por los Estados miembros de acuerdo con la Directiva 95/46/CE relativa a la protección de datos. Los ciudadanos podrán así presentar una denuncia directamente ante dicha autoridad si consideran que no se respetan los derechos protegidos por el Reglamento.

Cada institución y organismo comunitario designa al menos a una persona responsable de la protección de datos cuya función consiste en cooperar con el supervisor en la protección de datos y velar por que el tratamiento de datos no afecte negativamente a los derechos y libertades de las personas afectadas.

Este Reglamento permite a los ciudadanos gozar de derechos exigibles legalmente, como los de consulta, rectificación, bloqueo y supresión de los datos personales que consten en los archivos de cualquier institución u organismo de la Comunidad.

3.2 Marco español

3.2.1 La Constitución española

El derecho fundamental a la protección de datos personales reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos.

La Constitución Española reconoce en dos ocasiones el derecho fundamental a la protección de datos.

En su artículo 10 reconoce el derecho a la dignidad de la persona:

> *[1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.*
> *2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las materias ratificados por España.]*

Adicionalmente, en el artículo 18, se establece:

> *[1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
> *2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
> *4. 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.]*

Del conjunto de estos dos artículos es de donde ha derivado lo que hoy denominamos derecho a la protección de datos.

3.2.2 La Ley Orgánica 5/1992 (LORTAD)

Es la primera norma española específica para la protección de datos personales. La Ley Orgánica 5/1992 de 29 de octubre, Ley Orgánica de Regulación del Tratamiento Automatizado de los datos de carácter personal, conocida como LORTAD venía a desarrollar el artículo 18.4 de la Constitución Española.

En su exposición de motivos introduce otra serie de conceptos como son la "privacidad" como un concepto más amplio en referencia a la intimidad de las personas, la protección de sus datos de carácter personal y todo un conjunto de información que permita obtener un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

[El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona - el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.]

En la actualidad se encuentra derogada, cabe destacar que, su ámbito de aplicación se circunscribía únicamente a los ficheros de carácter personal que se tratan en soportes automatizados.

La Ley Orgánica de Protección de Datos vigente, conserva su estructura, si bien se introducirán las novedades oportunas para adaptar la normativa española a las exigencias de la Unión Europea.

3.2.3 Real Decreto 994/1999 de 11 de junio.

El Reglamento de Medidas de Seguridad aprobado mediante el Real Decreto 994/1999 tuvo por objeto el desarrollo de lo dispuesto en los artículos 9 y 43.3.h de la Ley Orgánica 5/1992. En la actualidad se encuentra derogado.

Tal y como establece en el artículo 9 de la Ley Orgánica 5/1992:

[1. El responsable del fichero deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza .de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natura1.
2. No se registrarán datos de carácter personal en ficheros automatizados que no reúnan las condiciones que se determinen por vía reglamentaria can respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones 9ue deban reunir los .ficheros automatizados y las personas que Intervengan en el tratamiento automatizado de los datos a que se refiere el artículo 7 de esta Ley.]

Y en su artículo 43.3. h):

[h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de segundad que por vía reglamentaria se determinen.]

De esta forma, el Reglamento venía a establecer las medidas de índole técnica y organizativa que garanticen la confidencialidad e integridad de la información con la finalidad de preservar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos personales frente a su alteración, pérdida, tratamiento o acceso no autorizado.

Las medidas de seguridad que se establecen se configuran como las medidas básicas de seguridad que han de cumplir todos los ficheros que contengan datos de carácter personal, sin perjuicio de establecer medidas especiales para aquellos ficheros que por la especial naturaleza de los datos que contienen o por las propias características de los mismos exigen un grado de protección mayor.

El Reglamento en su artículo 3 establece los diferentes niveles de seguridad: básico, medio y alto, en el artículo 4 establece la correspondencia entre los niveles mínimos de seguridad exigibles y los diferentes tratamientos de datos:

- Todos los ficheros que contengan datos de carácter personal deberán adoptar las medidas de seguridad calificadas como de nivel básico.

- 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.

- 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.

- Cuando los ficheros contengan un conjunto de datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo deberán garantizar las medidas de nivel medio establecidas en los artículos 17, 18, 19 y 20.

- Así, por ejemplo: un curriculum vitae, permitiría obtener más información de la persona tal y como se indica en el Reglamento, por lo que le serían de aplicación los artículos anteriormente citados.

Dentro de las medidas de seguridad exigibles en este Reglamento se encuentran:

- Medidas de Seguridad de nivel básico:
  - Documento de Seguridad
  - Funciones y obligaciones del personal
  - Registro de Incidencias
  - Identificación y autenticación
  - Control de acceso
  - Gestión de soportes
  - Copias de respaldo y recuperación

- Medidas de Seguridad de nivel medio:
  - Aspectos adicionales a incluir en el Documento de Seguridad
  - Existencia de un Responsable de seguridad.
  - Exigencia de realización de una Auditoría con carácter bienal.
  - Identificación y autenticación.
  - Medidas de control de acceso físico
  - Establecimiento de un registro de entrada y salida de soportes.
  - Información a incluir en el Registro de Incidencias
  - Pruebas con datos reales

- Medidas de Seguridad de nivel alto:
  - Cifrado en la distribución de soportes.
  - Establecimiento de un Registro de accesos a la información incluyendo determinada información y el detalle de los registros accedidos o a los que el acceso ha sido denegado.
  - Conservación de una copia de respaldo y recuperación en una ubicación alternativa.
  - Cifrado de las Telecomunicaciones.

3.2.4 Ley Orgánica 15/1999 del 13 de diciembre (LOPD)

El 14 de enero de 2000, se derogó la LORTAD y entró en vigor la Ley Orgánica de Protección de Datos de carácter personal, Ley 15/1999 de 13 de diciembre, cuyo objetivo es, tal y como se establece en su artículo 1:

[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.]

Esta ley está formada por 49 artículos distribuidos en 7 títulos, a continuación se describe qué información contiene cada uno de ellos.

3.2.4.1 Título I. Disposiciones generales

Se establece el objeto de la Ley y el ámbito de aplicación. Dentro del artículo relativo a definiciones se establecen los conceptos principales de datos de carácter personal, fichero, tratamiento de datos y entre otros, las figuras del responsable del fichero y el responsable del tratamiento.

3.2.4.2 Título II. Principios de la protección de datos

Se establecen los principios básicos relativos a:

- Calidad de datos
- Derecho de información en la recogida de datos
- Consentimiento
- Tratamientos de Datos especialmente protegidos
- Datos relativos a salud.
- Seguridad de los datos: se establece que el responsable del fichero y encargado del tratamiento deben adoptar un conjunto de medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.
- Deber de Secreto:
  Por el que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional y por tanto, a guardar la confidencialidad de la información y al deber de no divulgar esta información. Esta obligación se extiende aún después de finalizar la relación con el titular del fichero.
- Comunicación de los datos
- Acceso a los datos por cuenta de terceros. Tal y como se establece en el artículo 12 de la LOPD, la realización de tratamientos por cuenta de terceros debe estar regulada 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 tratamiento, 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.

  En el contrato se deben incluir también las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.

3.2.4.3 Título III. Derechos de las personas

En este título se establecen los principios relativos a los derechos de las personas:

- Derecho de consulta al Registro General de Protección de Datos, para obtener información acerca de la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento.

- Derecho de acceso: El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevé hacer de los mismos.

  Se proporcionará al interesado mediante su visualización, o mediante escrito, copia, o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

- Derecho de rectificación y cancelación: Los datos del interesado serán rectificados o cancelados, en su caso, cuando su tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

  La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

  Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

- Procedimiento de oposición, acceso, rectificación o cancelación: en el que se indica que existirán procedimientos establecidos reglamentariamente y que, además no existirá contra prestación alguna por el ejercicio de los derechos.

3.2.4.4 Título IV. Disposiciones sectoriales

En relación a las disposiciones sectoriales en este título se incluyen aspectos relativos a la gestión de ficheros de titularidad pública y titularidad privada; creación, modificación o supresión, comunicación de datos y excepciones particulares.

De forma particular se describe la existencia de los códigos tipo, entendidos como códigos deontológicos o de buena práctica profesional, consisten en acuerdos sectoriales a los que se pueden adherir las empresas que establecen las obligaciones, régimen de funcionamiento o los procedimientos de aplicación de la relación de empresas que se han adherido a los mismos.

3.2.4.5 Título V. Movimiento Internacional de Datos

En relación al movimiento internacional de datos, se establece que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable.

En particular, lo que se establece es que se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Existen determinadas excepciones, a lo indicado en los anteriores párrafos y que permiten excluir su aplicación en determinados casos.

3.2.4.6 Título VI. Agencia Española de Protección de Datos

Dentro de este título se incluyen los aspectos respecto a las funciones de la Agencia Española de Protección de Datos, las responsabilidades del Director, así como la estructura de los órganos autonómicos.

3.2.4.7 Título VII. Infracciones y sanciones

Dentro de este título se establecen los tipos de infracciones y sanciones, así como el procedimiento sancionador; dentro de este título se establecen la graduación de las sanciones en: leves, graves y muy graves.

3.2.5 Real Decreto 1720/2007 de 21 de diciembre

El Real Decreto 1720/2007 de 21 de diciembre, entró en vigor el 19 de abril de 2008, derogando el Reglamento de Medidas de Seguridad del Real Decreto 994/1999 que, en virtud de la Disposición Transitoria Tercera de la LOPD, había sido hasta la fecha la normativa de aplicación en relación con las medidas de seguridad.

El Reglamento de desarrollo de la LOPD regula, en su Título VIII, las medidas organizativas y técnicas que deben cumplir los ficheros y tratamientos que contengan datos de carácter personal, tanto automatizados como no automatizados, siendo en la actualidad la normativa de obligado cumplimiento en materia de protección de datos.

La necesidad de un Reglamento específico para la LOPD se hacía evidente, por varios motivos:

- El Reglamento hasta la fecha, se elaboró como Reglamento de la ley LORTAD.
- Ambigüedades en la interpretación de algunas de las medidas de seguridad en la aplicación de los ficheros.

- Hasta ese momento no se encontraban establecidas las medidas de seguridad de los ficheros que contienen datos de carácter personal y que no sean almacenados en ficheros automatizados, por ejemplo archivos y fuentes de documentación.

3.2.6 Sentencias Tribunal Constitucional 290/2000 y 292/2000

La sentencia 292/2000, de 30 de noviembre del Tribunal Constitucional, supone una evolución de la jurisprudencia constitucional para el reconocimiento de la autonomía del derecho a la protección de datos.

La sentencia se decanta por la diferenciación entre el derecho fundamental a la protección de datos y el derecho a la intimidad, en el último párrafo del Fundamento Jurídico 5. Establece que:

[Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.]

En el primer párrafo de su Fundamento Jurídico 6:

[6. La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin.]

Y en el párrafo tercero del Fundamento Jurídico 6:

[De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial,

sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.]

Por otro lado, la sentencia 292/2000, el Tribunal Constitucional declaró inconstitucionales y nulos el inciso "cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso o" del apartado 1 del artículo 21, y los incisos "impida o dificulte gravemente el cumplimiento de la funciones de control y verificación de las Administraciones públicas" y "o administrativas" del apartado 1 del artículo 24, y todo el apartado 2 de dicho artículo.

De esta forma, el Tribunal Constitucional viene a establecer el derecho a la protección de datos como derecho fundamental autónomo, cuyo contenido está integrado por los principios y derechos que se contemplan en la Ley Orgánica 15/1999. En virtud de este derecho fundamental, el ciudadano, con carácter general, puede decidir sobre sus propios datos.

3.3 Descripción detallada del Reglamento Real Decreto 1720/2007

El 21 de diciembre de 2007 el Consejo de Ministros aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que fue publicado en el Boletín Oficial del Estado número 17, del 19 de Enero, como Real Decreto 1720/2007.

En los siguientes apartados vamos a llevar a cabo una descripción y una interpretación de los aspectos que habría que tener en consideración en el entendimiento de la normativa.

3.3.1 Título I. Disposiciones generales

El Título I, además de establecer el objeto y ámbito de aplicación de la norma, contiene las definiciones que deben servir para centrar los conceptos.

Artículo 1. Objeto.
Donde se indica el objeto del RLOPD que es el Desarrollo de la LOPD.

Artículo 2. Ámbito objetivo de aplicación.
Considero importante destacar varios conceptos claves en relación al ámbito de cumplimiento:

- El Reglamento es 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.

- No es aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.
  De esta forma quedan excluidos, por ejemplo, los datos que se disponen en relación a las tarjetas de visita o información de contactos empresariales, siempre y cuando la información que se disponga únicamente sean los datos que cita la normativa.

- No es de aplicación a los datos referidos a personas fallecidas.
  Sí es necesario tener en cuenta, que el resto de contactos, familiares y demás figuras en relación a la posible comunicación de las personas fallecidas, sí será de aplicación.

Artículo 3. Ámbito territorial de aplicación.

En relación al ámbito territorial es necesario tener en cuenta que, se deben regir por este RLOPD los siguientes casos:

- Cuando el tratamiento sea efectuado en el marco de las actividades de una compañía que se encuentre ubicada en territorio español.

- Cuando no resulte de aplicación lo anterior, pero la compañía disponga de un encargado del tratamiento que sí está ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

- Cuando la compañía no esté establecida en territorio español, pero le sea de aplicación la legislación española, según las normas de Derecho internacional público.

- Cuando la compañía no esté establecida en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

Artículo 4. Ficheros o tratamientos excluidos.

No será de aplicación a determinados tratamientos y/o ficheros:

- Tratamientos realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas dentro del marco de la vida privada.
  Es decir, las propias agendas y/o dispositivos personales utilizados en el marco de la vida privada.

- Tratamientos sometidos a la normativa sobre protección de materias clasificadas.

- Tratamientos para la investigación del terrorismo y de formas graves de delincuencia organizada.

  Si bien, sí existen responsabilidades a cumplir por el responsable del fichero, como la comunicación previa de la existencia del fichero, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. Definiciones.

Las definiciones están a su vez divididas en dos apartados: el primero de ellos lo podemos considerar como definiciones generales a los efectos del Reglamento y el segundo se puede considerar como definiciones específicas que se concretan en lo contemplado en el Título VIII centrado exclusivamente en las medidas de seguridad en el tratamiento de los datos de carácter personal, con independencia de que se trate de ficheros automatizados o no automatizados.

Conceptos definidos por la LOPD:

1. Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.

   En este sentido la Agencia Española de Protección de Datos (en adelante AEPD) ha resuelto algunas dudas en relación a:
   - Datos de contactos de personas físicas de proveedores.

   - Direcciones de correo electrónico
     El dato de correo electrónico se considerará dato de carácter personal en función de cómo esté configurado. Si el usuario designa el correo electrónico utilizando su nombre y apellidos sí sería considerada como dato de carácter personal puesto que es posible vincular la dirección de correo electrónica con la persona titular de la misma. En principio si la cuenta ha sido configurada como un alias no podría vincularse a la persona física y por tanto no tendría consideración de dato de carácter personal

   - Imagen y sonido
     Los datos de imagen y sonido se regulan en la instrucción 1/2006 de la Agencia Española de Protección de Datos, en esta instrucción se establece que tendrán en consideración todos los aspectos que puedan identificar a una persona incluido su voz o su imagen.

2. Fichero: Todo conjunto organizado de datos de carácter personal cualquiera fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

   La normativa en materia de protección de datos es de aplicación tanto a ficheros total o parcialmente informatizados, como a ficheros en soporte papel.

3. 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.

4. Responsable del fichero o tratamiento: persona física o jurídica de naturaleza pública o privada u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento de los datos.

   Sobre el Responsable del fichero recaen las principales obligaciones establecidas por la LOPD, y le corresponde velar por el cumplimiento de la Ley. El responsable debe:

- Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.

- Asegurarse de que los datos sean adecuados y pertinentes, obtenidos de forma lícita y legítima y tratados de forma proporcional a la finalidad para la que fueron recabados.

- Garantizar el cumplimiento de los deberes de secreto y seguridad.

- Informar a los titulares de los datos personales en la recogida de éstos.

- Obtener el consentimiento para el tratamiento de los datos personales.

- Facilitar y garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

- Asegurar el cumplimiento de los aspectos exigidos en la LOPD en las relaciones con terceros.

- Cumplir con la legislación sectorial aplicable.

5. *Afectado o interesado*: persona física titular de los datos que sean objeto del tratamiento de datos.

6. Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a personas identificadas o identificables.

7. *Encargado del tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros trate datos personales por cuenta del Responsable del Fichero.

   La realización de un tratamiento por cuenta de terceros debe estar regulada 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 tratará los datos conforme a las instrucciones del responsable, que no lo aplicará o utilizará para fines distintos de los que figuren en dicho contrato, ni los comunicará, ni siquiera para su conservación, a terceros.

8. *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.

9. *Cesión o comunicación de datos*: toda revelación de datos realizada a una persona distinta del interesado.

10. *Fuentes accesibles al público*: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa sin más exigencia que en su caso el abono de una contraprestación.

Conceptos ampliados por el RLOPD:

1. *Cancelación*: procedimiento en virtud del cual el responsable del tratamiento cesa en el uso de los datos, e implica el bloqueo de los mismos.
   Dicho bloqueo consiste en impedir el acceso y el tratamiento de los datos, excepto para su puesta a disposición de las administraciones públicas, jueces y tribunales para la atención de las posibles responsabilidades nacidas del tratamiento y solo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

2. *Cesión o comunicación de datos*: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

3. *Consentimiento del interesado*: Toda manifestación de voluntad, libre, inequívoca, específica e informada mediante la que el interesado consiente el tratamiento de sus datos personales que le conciernen.

4. *Dato disociado*: aquel que no permite la identificación de un afectado o interesado.

5. *Datos de carácter personal*: cualquier información numérica, alfabética, gráfica, fotográfica, acústica, o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.
   Se establecen algunas excepciones al concepto de datos de carácter personal, regulados por el artículo 2.2, tal es el caso de los datos de contacto profesionales que quedan excluidos del ámbito de la LOPD.

6. *Datos de carácter personal relacionados con la salud*: las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo; en particular se consideran datos relacionados con la salud de un individuo los referidos a su porcentaje de discapacidad y a su información genética.

7. *Destinatario o cesionario*: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos. Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

8. *Encargado del tratamiento:* la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del Responsable del Tratamiento o Responsable del Fichero, como consecuencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

9. *Exportador de datos personales:* la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el Reglamento de la LOPD, una transferencia internacional de datos de carácter personal a un país tercero.

10. *Fichero:* todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

11. *Fichero no automatizado*: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.

12. *Importador de datos personales*: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea Responsable del Tratamiento, Encargada de Tratamiento o tercero.

13. *Persona identificable:* toda persona cuya entidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionadas para su averiguación.

14. *Procedimiento de disociación:* Todo tratamiento de datos personales que permita la obtención de datos disociados.

15. *Responsable del fichero o tratamiento:* Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

16. *Tercero*: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado y del interesado, del Responsable del Tratamiento, del Responsable del Fichero, del Encargado del Tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del Responsable del Tratamiento o del Encargado del Tratamiento.

17. *Trasferencia internacional de datos:* Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del Responsable del Fichero establecido en territorio español.

El Espacio Económico Europeo está formado por los países de la Unión Europea y los países miembros de la Asociación Europea de libre comercio, con excepción de Suiza.

18. *Tratamiento de datos:* cualquier operación o procedimiento técnico, sea o no automatizado, que implique la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, bloqueo o cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Artículo 6. Cómputo de plazos.

Se establecen las normas en referencia al cómputo de plazos, necesarios para el cumplimiento de los plazos establecidos, por ejemplo, en los ejercicios de Derechos de Acceso, Rectificación, Cancelación u Oposición.

Tal y como establece el RLOPD, para los plazos marcados por días se computarán únicamente los días hábiles; y cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. Fuentes accesibles al público.

Dado que las fuentes accesibles al público, tienen algunas consideraciones particulares, es necesario establecer cuáles son las fuentes consideradas como accesibles al público:

- El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.
- Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.
- Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.
- Los diarios y boletines oficiales.
- Los medios de comunicación social.

3.3.2 Título II. Principios de la protección de datos

3.3.2.1 Capítulo I. Calidad de los Datos

De conformidad con lo establecido en el artículo 4 de la LOPD:

> *[Los datos de carácter personal solo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación al ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.]*

En el artículo 8 del RLOPD, se desarrollan estos aspectos, siendo necesario tener en cuenta que:

- los datos personales no podrán utilizarse para finalidades incompatibles a aquellas para las que hubieran sido recogidos. El responsable del fichero no debe recoger datos que no sean necesarios para atender la finalidad determinada en el momento de la recogida.

  Es necesario tener en cuenta que no se considera incompatible el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

- serán exactos, actualizados y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

  Siempre que los datos se recojan directamente del afectado se presumirá que los mismos son exactos.

  Se establece un plazo de 10 días para la actualización, rectificación de los datos que resulten inexactos a partir del momento en el que se conozca dicha inexactitud; si los datos hubieran sido comunicados se procederá a comunicarlo a los distintos cesionarios dentro del mismo plazo. De la misma forma el cesionario dispondrá de un plazo de 10 días para proceder a la corrección de los datos a partir de la recepción de la notificación.

- serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que fueron recabados y tratados.

  Si los datos han sido tratados dentro de una relación jurídica entre dos partes y existe la posibilidad de que se puedan derivar responsabilidades, los datos podrán ser conservados durante el plazo de prescripción de dichas responsabilidades.

- serán almacenados de forma que permitan el ejercicio de derechos de acceso.

- no podrán ser recogidos por medios fraudulentos, desleales o ilícitos. La licitud en la recogida implica cumplir con los siguientes aspectos:

  - Los datos han de recabarse de forma legal, siendo necesario el consentimiento del afectado, salvo que la Ley disponga otra cosa.
  - Los datos recabados deben ser necesarios para la realización del contrato o la actividad que justifique su recogida.
  - Los datos recabados deben utilizarse únicamente para la finalidad legítima para la que han sido recogidos.

Artículo 9. Tratamiento con fines estadísticos, históricos o científicos.

Se establece que no se considerará incompatible, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

También se establece como excepción a los criterios de cancelación, dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos.

Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos.

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando lo autorice una norma con rango de

ley o una norma de derecho comunitario y, en particular, cuando concurra determinados supuestos.

Se establece que los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

- Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

- Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

- El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

Se establece que la cesión de los datos de carácter personal podrá llevarse a cabo sin contar con el consentimiento del interesado cuando:

- La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

- La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

- La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:
    a. Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.
    b. Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.
    c. La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

En relación a los datos especialmente protegidos, se establece que podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre. En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas.

Artículo 11. Verificación de datos en solicitudes formuladas a las Administraciones públicas.
Este artículo regulaba la verificación de datos en solicitudes por medios electrónicos, si bien, fue anulado por disconforme a derecho, por Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo.

3.3.2.2 Capítulo II. Consentimiento para el tratamiento de los datos y Deber de Información

- *Sección I. Obtención del consentimiento del afectado*

Artículo 12. Principios generales.

De conformidad con lo establecido en el artículo 5 de la LOPD:

[1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:
a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b. Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e. De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b, c y d del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a, d y e del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.]

La simple inclusión de datos de carácter personal en un fichero supondrá un tratamiento de datos personales, que requiere, salvo en determinados casos, el consentimiento del afectado, teniendo en cuenta la definición de consentimiento como: "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el interesado consienta el tratamiento de datos personales que le conciernen":

- Libre: el consentimiento debe ser otorgado de forma libre por el propio interesado.

- Previo a la obtención de los datos del afectado, éste tendrá que ser informado, de modo expreso, preciso e inequívoco:
  a. De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información
  b. Del carácter obligatorio o facultativo de su respuesta, así como de las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  c. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

De conformidad con el artículo 6 de la LOPD en referencia al consentimiento:

[1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.]

En relación a la obtención del consentimiento para el tratamiento de datos de menores de edad, es necesario tener en cuenta que para llevar a cabo el tratamiento de datos de menores de 14 años será necesario el consentimiento de los padres o tutores. También se indica que la información que se facilite en relación al tratamiento de los datos debe expresarse en un lenguaje que sea fácilmente comprensible.

Es responsabilidad del responsable del fichero establecer mecanismos que permitan garantizar que éste ha verificado la edad del menor y la autenticidad del consentimiento otorgado por los padres, tutores o representantes legales.

Artículo 14. Forma de recabar el consentimiento.

Se establece que el responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 del Reglamento de Desarrollo de la LOPD y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

Esta forma de obtener el consentimiento solo será válida para aquellos casos en los que la LOPD no exige un consentimiento expreso para el tratamiento de los datos.

Se incluye de forma particular, para aquellos servicios que generen información periódica o reiterada, o facturación periódica, que la comunicación podrá llevarse a cabo

de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considera válido, entre otros, remitir un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

Como requisito, es necesario tener en cuenta que si el responsable ha solicitado de esta forma el consentimiento al afectado, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.

Es posible que el responsable del fichero, solicite el consentimiento al interesado para otras finalidades que no guarden relación directa con la misma (por ejemplo el envío de algún boletín, información comercial), en estos casos se establece que el responsable del fichero deberá describir todas las finalidades para las que se recogen los datos objetos de tratamiento y así mismo, establecer un mecanismo para que en ese primer momento el interesado pueda manifestar su oposición a estos otros fines.

Por ejemplo, el Reglamento establece como un medio válido, la implementación de una casilla que el interesado pueda marcar en el caso de aceptar dichas finalidades.

Artículo 16. Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. Revocación del consentimiento.

El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento, entre otros, entre otros, remitir un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o

envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento.

Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

Es importante tener en cuenta que, si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el mismo plazo de 10 días para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran.

- *Sección II. Deber de información al interesado*

Artículo 18. Acreditación del cumplimiento del deber de información.

Este artículo establecía la obligatoriedad de llevar a cabo el deber de información a través de un medio que permitiera la acreditación de haber llevado a cabo dicho deber de información y conservación de esta acreditación, si bien, fue anulado por disconforme a derecho, por Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo.

Artículo 19. Supuestos especiales.

En este artículo se establecen los supuestos especiales en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil; en estos supuestos se indica que no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

3.3.2.3 Capítulo III. Encargado del tratamiento

Artículo 20. Relaciones entre el responsable y el encargado del tratamiento.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido. Se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

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 considerado,

también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Artículo 21. Posibilidad de subcontratación de los servicios.

El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

Es posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que en el propio contrato se especifiquen los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

b) Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

c) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

d) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberá procederse a la autorización de dicha subcontratación.

Artículo 22. Conservación de los datos por el encargado del tratamiento.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

3.3.3 Título III. Derechos de acceso, rectificación, cancelación y oposición

El Título III está dedicado a los derechos de las personas y en particular a las disposiciones aplicables al ejercicio de los derechos de acceso, rectificación, cancelación y oposición. Se centra principalmente, en las características del derecho correspondiente, como ejercer dicho derecho, y el otorgamiento o la denegación del mismo.

3.3.3.1 Capítulo I. Disposiciones generales

Es necesario tener en cuenta que los derechos de Acceso, rectificación, cancelación y oposición siempre serán ejercidos por el propio interesado.

Para ello, deberá acreditarse su identidad o a través de su representante con la correspondiente acreditación.

En relación al ejercicio de los derechos se establece que son independientes, y que debe concederse un medio sencillo y gratuito para el ejercicio de alguno de ellos.

Para el ejercicio de los derechos debe implementarse un medio sencillo y gratuito para el ejercicio de los derechos por parte del interesado. También se establece que si la Entidad dispone de canales para su atención al público, que se puedan utilizar estos mismos mecanismos para el ejercicio de los derechos.

Se establece que para el ejercicio de derecho debe de adjuntarse fotocopia del documento nacional de identidad o pasaporte que permita la acreditación del interesado; la petición de ejercicio de derecho.

El responsable del fichero, a su vez, debe contestar la solicitud en todo caso y con los plazos de tiempo establecidos.

En relación a los interesados que se dirigen a un encargado del tratamiento, éste deberá solicitar la petición al responsable del fichero.

3.3.3.2 Capítulo II. Derecho de acceso

El Derecho de acceso es el derecho por el que el afectado puede obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

Este derecho podrá ser ejercido a través de varios medios:

- permitiendo la visualización en pantalla por parte del interesado.
- escrito, copia o fotocopia remitida por correo, certificado o no.
- telecopia.
- correo electrónico u otros sistemas de comunicaciones electrónicas.
- cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

El responsable del fichero deberá resolver esta solicitud en el plazo de un mes desde la recepción de la solicitud. La información proporcionada comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

El responsable del fichero podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.

Podrá denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3.3.3.3 Capítulo III. Derechos de rectificación y cancelación

El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo de los datos.

La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud, es necesario tener en cuenta que cuando el responsable no disponga de datos de carácter personal del afectado deberá igualmente comunicarlo en el mismo plazo.

De igual forma, si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en el mismo plazo, para que éste procesa asimismo, a rectificar o cancelar los datos.

La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

Podrán también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3.3.3.4 Capítulo IV. Derecho de Oposición

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a. Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b. Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

c. Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado.

3.3.4 Título IV. Disposiciones aplicables a determinados ficheros de titularidad privada

El Título IV está dedicado a cuestiones específicas aplicables a determinados ficheros de titularidad privada, como son los ficheros relativos a solvencia patrimonial y crédito, que se describe en el artículo 29 de la LOPD, así como tratamientos para actividades de publicidad y prospección comercial incluidos en el artículo 30 de la LOPD.

3.3.4.1 Capítulo I. Ficheros de información sobre solvencia patrimonial y crédito

Tratamientos de datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias

En relación a los tratamientos de datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés, se indica que estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado.

En cuanto al tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta, sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada.

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos anteriormente citados.

Información previa

Antes de la inclusión, el acreedor se debe informar al deudor de forma conveniente, para ello, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar un requerimiento de pago, que en el caso de no producirse dicho pago en los términos previstos para ello y cumplirse los requisitos anteriormente citados, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

De igual forma, el Responsable del Fichero debe notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, informando de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición. Esta notificación debe llevarse a cabo mediante un medio fiable y auditable, y el Responsable del Fichero debe disponer de la confirmación de que el interesado ha recibido dicha información.

Conservación de los datos

- Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.
  El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.
- En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Acceso a la información contenida en el fichero

- Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

  - Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.
  - Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.
  - Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

- Los terceros deberán informar por escrito a las personas en las que concurran los dos últimos supuestos contemplados en el apartado anterior, precedentes de su derecho a consultar el fichero.

Ejercicio de los derechos de acceso, rectificación, cancelación y oposición

Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero de cumplimiento o incumplimiento de obligaciones dinerarias se tendrán en cuenta las siguientes reglas:

- Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

  En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

- Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

  Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero de cumplimiento o incumplimiento de obligaciones dinerarias, se tendrán en cuenta las siguientes reglas:

- Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

- Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días.

- Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para que, en su caso, pueda ejercitar sus derechos ante el mismo.

3.3.4.2 Capítulo II. Tratamientos para actividades de publicidad y prospección comercial

Se establece que las Entidades que se dediquen a actividades de publicidad solo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a. Procedan de fuentes accesibles al público y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades concretas de publicidad y prospección comercial.

b. Hayan sido facilitados por los propios interesados contando con su consentimiento para finalidades determinadas relacionadas con la actividad de publicidad o prospección comercial.

Es necesario tener en cuenta que, cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, debe informarse al interesado en cada comunicación del origen de los datos y de la identidad del responsable así como de los derechos que le asisten y ante quién puede ejercitar los mismos.

Se establece que, en el caso de que una Entidad subcontrate a un encargado del tratamiento la realización de una determinada campaña publicitaria, habrá que determinan cual de las dos entidades será la responsable de dicho tratamiento:

- Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

- Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

- Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

También se establece la obligatoriedad del cumplimiento de los derechos ARCO en relación a la oposición de este tratamiento, indicándose también que los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

3.3.5 Título V. Obligaciones previas al tratamiento de los datos

El Título V se centra en los aspectos a tener en cuenta en relación a las obligaciones previas al tratamiento de los datos. Como responsabilidades se establece la creación, modificación o supresión de ficheros ya sean de titularidad pública o privada (artículos 20 y 26 de la LOPD respectivamente).

3.3.5.1 Capítulo I. Creación, modificación o supresión de ficheros de titularidad pública

La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el Boletín Oficial del Estado o en el diario oficial correspondiente.

En relación al contenido de creación del fichero deberá contener:

a. La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b. El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c. Descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d. Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e. Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f. Los órganos responsables del fichero.

g. Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h. El nivel básico, medio o alto de seguridad que resulte exigible en función de los datos objetos de tratamiento.

Respecto a las modificaciones de los ficheros habrá que tener en cuenta que es necesario indicar las modificaciones producidas en el apartado correspondiente de la declaración del fichero.

Respecto a la supresión de los ficheros se establecerá cual es la acción a realizar con los datos, o, en su caso la destrucción de los mismos.

3.3.5.2 Capítulo II. Notificación e inscripción de los ficheros de titularidad pública o privada

Los ficheros de datos de carácter personal de titularidad pública deben ser notificados a la Agencia Española de Protección de Datos por el órgano competente del Responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

Los ficheros de datos de carácter personal de titularidad privada deben ser notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación.

La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, el nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la AEPD o a las autoridades de control autonómicas competentes.

La inscripción del fichero contiene el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad correspondiente, en su caso se incluirá la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

3.3.6 Título VI. Transferencias internacionales de datos

El Título VI está dedicado a las transferencias internacionales de datos (correspondiente con los artículos 33 y 34 de la LOPD), estableciéndose aspectos concretos en el caso de que la transferencia se realice a estados con nivel adecuado de protección o no.

3.3.6.1 Capítulo I. Disposiciones generales

Se establece la obligatoria autorización y notificación a la AEPD de la transferencia internacional, la autorización será requerida para todos los casos exceptuando:

a. Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II del RLOPD.

b. Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a. a j. del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3.3.6.2 Capítulo II. Transferencias a estados que proporcionen un nivel adecuado de protección

Se establece que no será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

La Agencia Española de Protección de Datos mantiene la relación actualizada de países cuyo nivel de protección haya sido considerado equiparable.

El Director de la AEPD, podrá establecer la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a. Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b. Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

3.3.6.3 Capítulo III. Transferencias a estados que no proporcionen un nivel adecuado de protección

Se establece que cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

El Director de la Agencia Española de Protección de Datos podrá denegar o suspender temporalmente la transferencia, cuando concurra alguna de las circunstancias siguientes:

a. Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b. Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c. Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d. Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e. Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

3.3.7 Título VII. Códigos Tipo

El Título VII está dedicado a lo que se denominan los códigos Tipo (correspondiente con el artículo 32 de la LOPD), contemplando sus particulares características respecto a su objeto y naturaleza, contenido y compromisos adicionales; así como aspectos relacionados como son las garantías de cumplimiento o el depósito y publicación de estos Códigos Tipo.

Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

Los códigos tipo tienen el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Dentro de este título, se incluye la información que debe contener el código tipo, existiendo la información mínima obligatoria que deberán contener y adicionalmente otras de carácter voluntario.

Dentro de este título se establece también la evaluación periódica de la eficacia del Código Tipo, midiendo el grado de satisfacción de los afectados; teniendo que realizarse esta evaluación cada cuatro años.

3.3.8 Título VIII. De las medidas de seguridad en el tratamiento de datos de carácter personal

En el Título VIII se establecen las medidas de seguridad que se deberán implementar para cada uno de los ficheros que contengan datos de carácter personal en función de que dichos datos correspondan a nivel básico, medio o alto.

Igualmente, en este Título se distinguirán las medidas que es necesario cumplir sean ficheros automatizados o ficheros no automatizados.

Se analizará en detalle en el siguiente capítulo de este proyecto.

3.3.9 Título IX. Procedimientos tramitados por la Agencia Española de Protección de Datos

El Título IX contempla los procedimientos que se tramitan en la Agencia Española de Protección de Datos, respecto al procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición; procedimientos relativos al ejercicio de la potestad sancionadora; así como procedimientos relativos a la inscripción o cancelación de ficheros y/o códigos Tipo.

Capítulo 4

La Agencia Española de Protección de Datos

4.1 Introducción

La Agencia Española de protección de datos es el órgano de control del cumplimiento de la Ley, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Regulada por:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria).

- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

Fue creada por la LORTAD y regulada en la vigente LOPD, la Agencia se muestra como la instancia a la que pueden acudir los afectados para ser tutelados en el ejercicio de sus derechos.

Por su parte, el Consejo Consultivo es un órgano colegiado de asesoramiento al director de la AEPD, que emite aquellos informes sobre las cuestiones que le sean solicitadas por éste.

El Registro General de Protección de Datos tiene como principal función la de velar por la publicidad de los tratamientos de datos. Tramita expedientes relacionados con la inscripción de tratamientos notificados, la autorización de transferencias internacionales de datos y la inscripción de códigos tipo; es un registro declarativo que inscribe ficheros públicos y privados.

El órgano de Inspección de Datos, que tiene como función comprobar la legalidad de los tratamientos efectuados por los responsables de los ficheros. Los inspectores, dada su naturaleza de autoridad pública, instruyen los procedimientos y pueden actuar ante una denuncia de un afectado o bien dentro de una inspección de oficio
.

La Secretaría General de la AEPD persigue y apoya el adecuado funcionamiento de la AEPD, gestiona el fondo de documentación, edita la memoria de la AEPD, así como otras publicaciones, prepara eventos y conferencias y procede a la atención al ciudadano en sus dudas y cuestiones planteadas en relación con la protección de datos de carácter personal.

La Agencia está dirigida por el Director, quien ostenta también su representación, será nombrado de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años, teniendo la consideración de “alto cargo”.

4.2 Funciones de la Agencia Española de Protección de Datos

Las funciones de la Agencia de protección de datos podrían resumirse en función de la naturaleza de las mismas como:

Las funciones que se encomiendan en virtud del artículo 37 de la LOPD son:

a. Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c. Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la Ley.

d. Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f. Requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la Ley, y en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.

g. Ejercer la potestad sancionadora en los términos previstos por el Título VII de la Ley Orgánica 15/1999.

h. Informar con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley.

i. Recabar de los responsables de los ficheros cuanta ayuda e información estimen necesaria para el desempeño de sus funciones.

j. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k. Redactar una memoria anual y remitirla al Ministerio de Justicia.

l. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos.

m. Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere la Ley en su caso.

n. Otras establecidas por normas legales o reglamentarias.

4.3 Las Agencias de Protección de Datos Autonómicas

La LOPD establece en su artículo 41, la existencia de Agencias de Protección de Datos Autonómicas:

[1. Las funciones de la Agencia Española de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j, k y l, y en los apartados f y g en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.
2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.
3. El Director de la Agencia Española de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia Española de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.]

Dichas Agencias ejercerán las mismas funciones que la Agencia Española de Protección de Datos salvo las que se muestran en la siguiente tabla:

Funciones establecidas en la LOPD, artículo 37.1	AEPD	Órganos Autonómicos
a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.	Sí	Sí
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.	Sí	Sí
c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la Ley.	Sí	Sí
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.	Sí	Sí
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.	Sí	Sí
f) Requerir a los responsables y los encargados de los tratamientos la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de la Ley, y en su caso, ordenar la cesación de los tratamientos y la cancelación de	Sí	No en lo que se refiera a transferencia internacional de datos

Funciones establecidas en la LOPD, artículo 37.1	AEPD	Órganos Autonómicos
los ficheros, cuando no se ajuste a sus disposiciones.		
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la Ley Orgánica 15/1999.	Sí	No en lo que se refiera a transferencia internacional de datos
h) Informar con carácter preceptivo, los proyectos de disposiciones generales que desarrollen la Ley.	Sí	Sí
i) Recabar de los responsables de los ficheros cuanta ayuda e información estimen necesaria para el desempeño de sus funciones.	Sí	Sí
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.	Sí	No
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.	Sí	No
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos.	Sí	No
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere la Ley en su caso.	Sí	Sí, salvo en lo que se refiere al artículo 46 de la LOPD
n) Otras establecidas por normas legales o reglamentarias.	Sí	Sí

Tabla 1: Funciones comparación autoridades de control

4.3.1 Autoridad Catalana de Protección de Datos

Se rige por la Ley 5/2002, de 19 de abril, de la Autoridad Catalana de Protección de Datos de carácter personal, que establece sus funciones:

- Velar por el cumplimiento de la legislación vigente sobre protección de datos de carácter personal y controlar su aplicación.

- Velar por el cumplimiento de las disposiciones que la Ley de Estadística de Cataluña establece respecto a la recogida de datos estadísticos y al secreto estadístico, y adoptar las medidas correspondientes para garantizar las condiciones de seguridad de los ficheros constituidos con finalidades exclusivamente estadísticas, salvo lo que se refiere a las transferencias internacionales de datos.

- Dictar las instrucciones necesarias para adecuar los tratamientos de datos personales a los principios de la legislación vigente.

- Requerir a los responsables y a los encargados del tratamiento la adopción de las medidas necesarias para la adecuación del tratamiento de datos personales objeto de investigación a la legislación vigente en materia de protección de datos de carácter personal, y en su caso, ordenar el cese de los tratamientos y la cancelación de los ficheros, excepto en lo que se refiere a las transferencias internacionales de datos.

- Proporcionar información sobre los derechos de las personas y atender a sus peticiones y reclamaciones.

- Obtener de los responsables de los ficheros la ayuda y la información que consideren necesarias para el ejercicio de sus funciones.

- Ejercer la potestad de inspección excepto en lo que se refiere a las transferencias internacionales de datos.

- Ejercer la potestad sancionadora que tiene encomendada.

- Informar, con carácter preceptivo, sobre los proyectos de disposiciones de carácter general de la Generalitat de Cataluña en materia de protección de datos de carácter personal.

- Responder a consultas que la Administración de la Generalitat, los entes locales y las universidades de Cataluña le formulen y colaborar con ellas en la difusión de las obligaciones establecidas.

La Agencia Catalana de protección de datos se compone de: Dirección, Secretaría General, Asesoría Jurídica, Área de Inspección, Área de Registro y Coordinación de las nuevas tecnologías y sociedad de la información.

4.3.2 Agencia Vasca de Protección de Datos

La normativa reguladora es la Ley 2/2004 de 25 de febrero, las funciones que se establecen son las siguientes:

- Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.

- Emitir las autorizaciones previstas en las leyes y reglamentos.

- Dictar las instrucciones precisas.

- Atender las peticiones y reclamaciones formuladas por los afectados y proporcionar información a las personas acerca de sus derechos.

- Requerir a los responsables y a los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a la legislación en vigor.

- Ejercer la potestad sancionadora.

- Informar, con carácter preceptivo, sobre los proyectos de disposiciones generales que desarrollen la ley.

- Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

- Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará anualmente una relación de dichos ficheros con la información adicional que el director de la Agencia Vasca de Protección de Datos determine.

- Redactar una memoria anual y remitirla a la vicepresidencia del Gobierno vasco.

- Velar por el cumplimiento de las disposiciones que la legislación sobre la función estadística pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas y dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos.

- Colaborar con la Agencia Española de Protección de Datos y entidades similares de otras comunidades autónomas.

- Atender a las consultas que en materia de protección de datos de carácter personal le formulen las administraciones públicas, instituciones y corporaciones, así como otras personas físicas o jurídicas.

En cuanto a su estructura, la Agencia Vasca de Protección de Datos se compone de un órgano unipersonal (director) y un órgano colegiado (Consejo Consultivo). Jerárquicamente dependen del director el Registro de Protección de Datos y Nuevas Tecnologías, la Asesoría Jurídica e Inspección y la Secretaría General.

4.4 La actividad inspectora y sancionadora de la AEPD

4.4.1 Función inspectora

La AEPD como autoridad de control tiene encomendada, entre otras funciones, la potestad de inspeccionar aquellas actividades en los que existan o puedan existir indicios una vulneración de la normativa sobre la que es competente.

Para ello, y antes de iniciar un procedimiento sancionador, la AEPD inicia una serie de actuaciones previas dirigidas a investigar si los hechos o actividades denunciadas son constitutivos de delito.

Si durante estas investigaciones la AEPD encuentra indicios de hechos sancionables, se iniciará un procedimiento sancionador para investigar más en detalle los hechos o actividades denunciadas y sancionarlos si fuera procedente.

A continuación en el siguiente gráfico se muestran los procedimientos relativos al ejercicio de la potestad sancionadora iniciados por la AEPD en los tres últimos años:

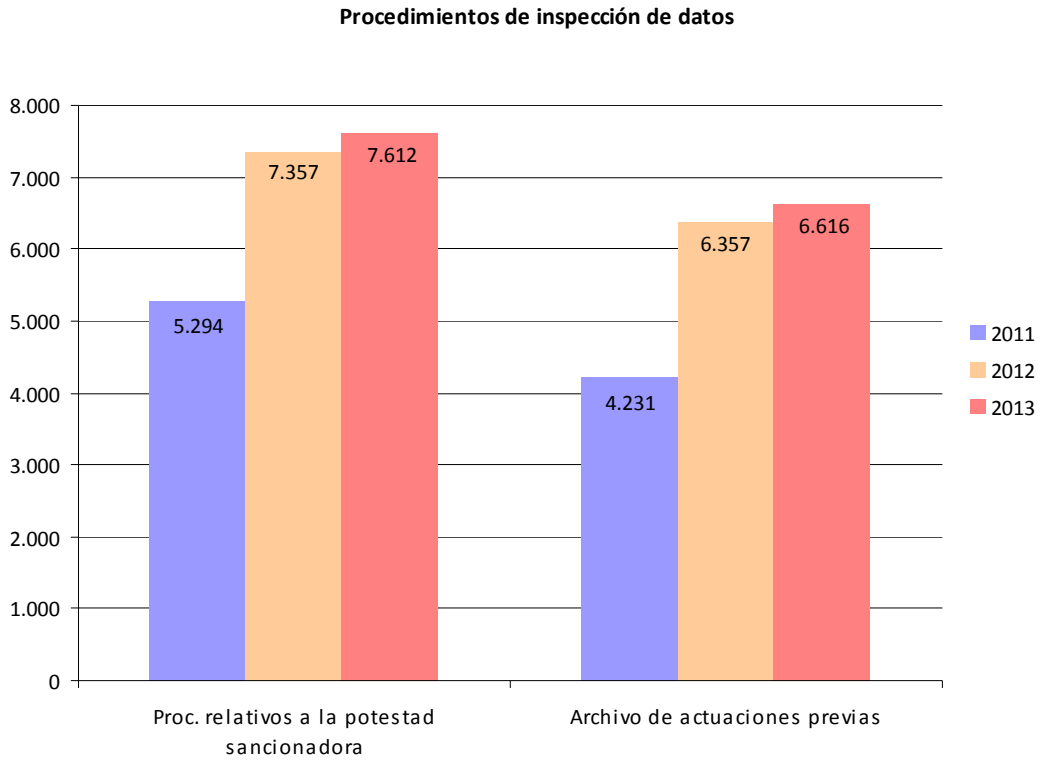


Figura 2: Procedimientos de inspección de datos Memorias AEPD 2011, 2012 y 2013

Del total de las inspecciones realizadas por la AEPD, con respecto a la normativa sobre protección de datos, cabe señalar lo siguiente:

- Que ha existido un mantenimiento en la apertura de procedimientos sancionadores respecto al año pasado (incremento 3,47%)
- Que el número de archivo de actuaciones previas se ha mantenido respecto al año pasado (incremento 4%)

A continuación se muestra un gráfico en el cual se detalla el resultado de los procedimientos sancionadores resueltos por la AEPD en los tres últimos años:

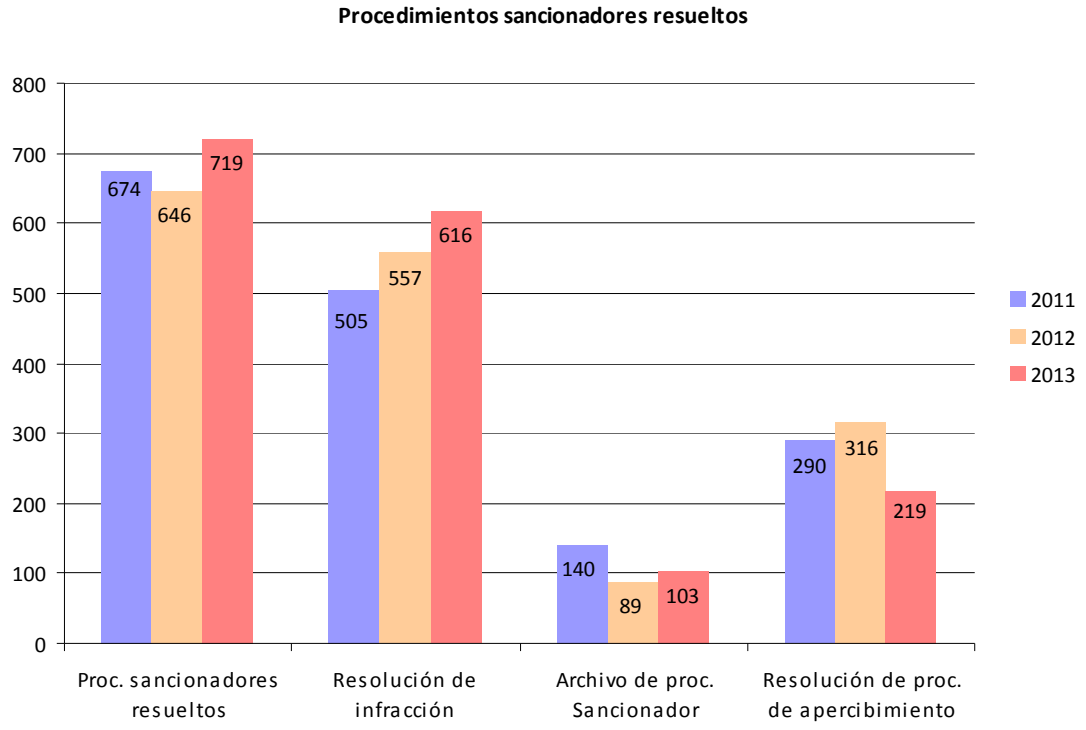


Figura 3: Procedimientos Sancionadores Memorias AEPD 2011, 2012 y 2013

De los procedimientos sancionadores resueltos por la AEPD cabe señalar lo siguiente:

- El número total de procedimientos sancionadores se ha incrementado un 11,30%.
- El número de procedimientos sancionados ha aumentado un 10,60%.
- El número de procedimientos archivados ha aumentado un 15,73%.
- El número de procedimientos de apercibimiento ha disminuido un 30,70%

4.4.2 Función sancionadora

Una de las funciones que tiene la AEPD es la de vigilar el cumplimiento de las normativas relacionas con la protección de datos, con los servicios de la sociedad de la información y los relacionados con las telecomunicaciones.

A continuación se muestra la actividad sancionadora que ha venido realizando la AEPD durante los tres últimos años, con respecto a la vigilancia y control de la normativa que es de su competencia:

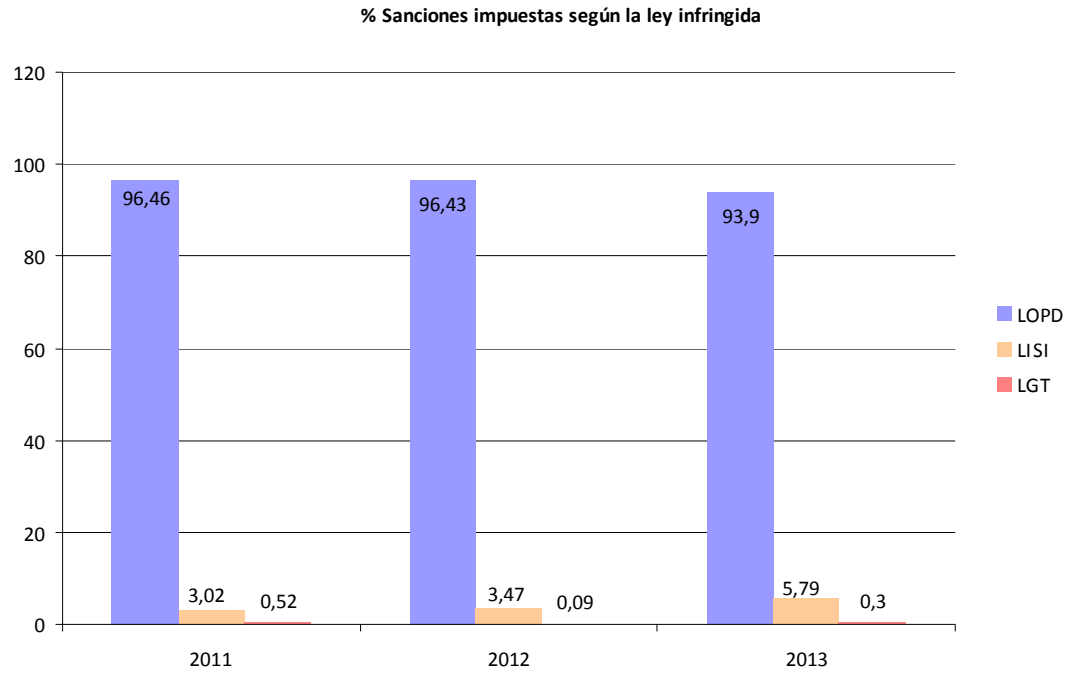


Figura 4: %Sanciones Memorias AEPD 2011, 2012 y 2013

A la vista de estos datos, llama la atención:

- El elevado porcentaje de sanciones impuestas en materia de protección de datos con respecto a las otras normativas competencia de la AEPD y mantenimiento de esta cifra respecto a años anteriores.
- Incremento de las sanciones relativas a LSSI respecto al año anterior.
- Que la mayor parte de la actividad de la AEPD se desarrolla sobre la normativa de protección de datos.

Se puede comprobar que aunque la AEPD tiene competencias sobre varias materias, principalmente centra su actividad en materia de protección de datos.

Dentro de esta potestad sancionadora que tiene la AEPD, existe una graduación de sanciones tipificadas en función al hecho que origine el incumplimiento de la normativa.

En la tabla siguiente se muestran los grados de las sanciones impuestas en los tres últimos años:

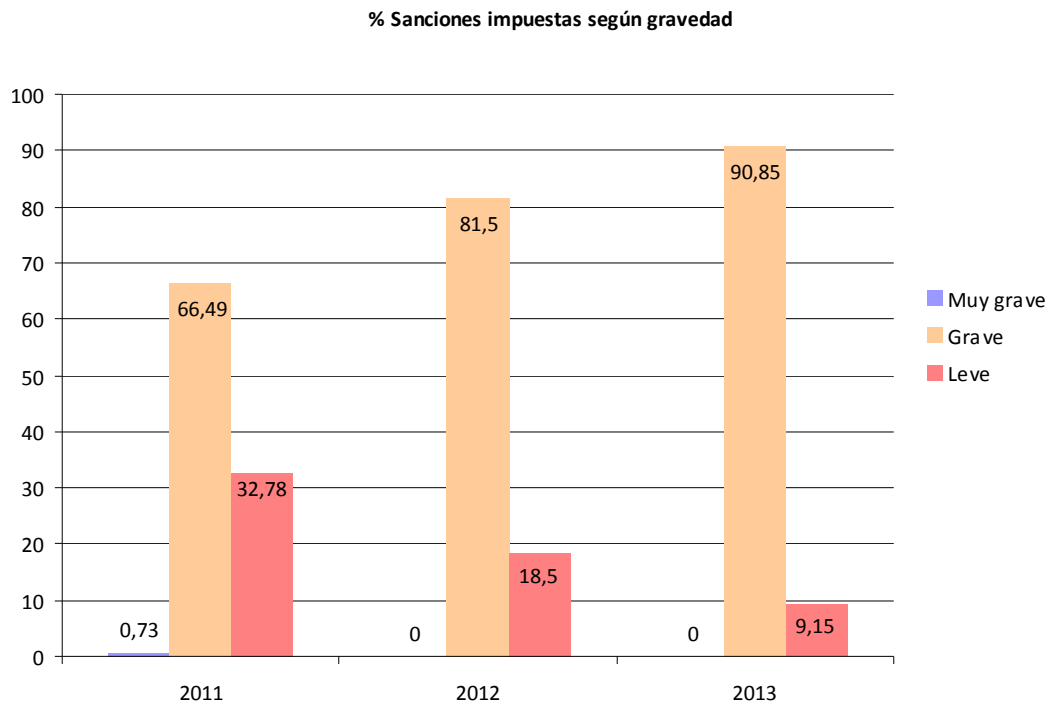


Figura 5: %Sanciones impuestas según gravedad Memorias AEPD 2011, 2012 y 2013

Del análisis de estos datos cabe destacar:

- El mantenimiento en los últimos años de pocas sanciones muy graves.
- El incremento de sanciones graves con respecto al año anterior.
- El decremento respecto de las sanciones leves del año anterior.

4.5 Sentencias de la Audiencia Nacional y del Tribunal Supremo

Las resoluciones impuestas por los procedimientos sancionadores de la AEPD ponen fin a al vía administrativa, por este motivo, en el caso de no estar conforme con la resolución impuesta podrá recurrirse ante los tribunales de justicia.

El órgano encargado de revisar las Resoluciones de la Agencia Española de Protección de Datos, en única instancia, es la Sala de lo Contencioso de la Audiencia Nacional, por lo que sus pronunciamientos son claves para poder entender, en cada momento y de forma evolutiva en el tiempo, la normativa sobre protección de datos de carácter personal, aunque también la Sala Tercera de lo Contencioso-Administrativo del Tribunal Supremo puede entrar a analizar cuestiones sobre esta normativa.

Este tribunal tiene como función volver a analizar todas las pruebas y documentación aportada en el procedimiento ante la AEPD, para emitir una nueva resolución en la que: se confirme la resolución dictada por la AEPD, se rechace, o se admitan ciertos aspectos y se rechacen otros.

Capítulo 5

Auditoría

5.1 Conceptos básicos

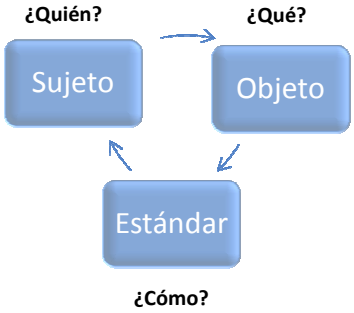
Este capítulo describe los conceptos básicos de Auditoría. Como primer aspecto, necesitamos partir de la definición de auditoría, por ello indicar que por auditoría entendemos:

- Una recopilación, acumulación y evaluación de evidencias sobre información de una entidad, para determinar e informar el grado de cumplimiento entre la información y los criterios establecidos.

- Una sistemática evaluación de las diversas operaciones y controles de una organización, para determinar si se siguen políticas y procedimientos aceptados, si se siguen las normas establecidas, si se utilizan los recursos eficientemente y si se han alcanzado los objetivos de la organización.

- Un proceso sistemático para obtener y evaluar de manera objetiva, las evidencias relacionadas con informes sobre actividades económicas y otras situaciones que tienen una relación directa con las actividades que se desarrollan en una entidad pública o privada. La finalidad del proceso consiste en determinar el grado de precisión del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso.

La auditoría es un proceso por el que se lleva a cabo por parte del sujeto (auditor) una revisión de un objeto (objeto a auditar: empresa, área, proceso..), con el fin de emitir una opinión acerca de su razonabilidad sobre la base de un patrón estándar establecido (punto de comparación para poder evaluar si la situación bajo examen cumple o no con el patrón establecido).



5.2 La figura del auditor

Por su parte, el auditor es una persona capacitada y con la suficiente experiencia para revisar y verificar que la información objeto de la auditoría cumple los estándares determinadas.

El auditor tiene que redactar un informe al concluir la auditoría determinando el grado de veracidad y claridad que la organización posee contablemente.

De entre las características que debe mostrar el auditor se encuentran:

- Formación y Capacidad Profesional
- Experiencia
- Independencia
- Integridad
- Objetividad
- Capacidad de análisis y síntesis
- Diligencia Profesional
- Responsabilidad
- Secreto Profesional

5.3 Tipos de auditoría

Existen diferentes tipos de auditoría, dado que pueden existir distintas en función de que es lo que se audite ó quién lleve a cabo esta auditoría ó el ámbito de la misma, en las siguientes tablas se incluye la clasificación realizada por los profesores J.L. Wanden-Berghe y J.A. Trigueros, donde se puede comprobar este hecho:

En función del ***sujeto:***	- que es auditado	Privada Pública Mixta
	- que realiza la auditoría	Interna Externa
En función de la ***actividad desarrollada***	De seguros Bancarias De inmobiliarias De extractoras De servicios Deportivas, etc.	
En función del ***objeto:***	Financiera Operativa o de gestión De sistemas Integral Social Medioambiental	
En función de la ***legalidad:***	Obligatoria Voluntaria	
En función del ***ámbito:***	Completa	
	Parcial o revisión limitada	De cumplimiento Informes especiales o de áreas concretas
En función de la ***temporalidad:***	De regularidad Esporádica	

Tabla 2: Tipos de auditorías

5.4 Auditoría Informática

En concreto la Auditoría Informática conlleva el proceso de recoger, analizar y realizar una evaluación de las evidencias para determinar si un sistema de información cumple los aspectos normativos y/o los requerimientos funcionales para los que fue diseñado.

A su vez, la auditoría informática puede ser de varias tipos, en función del objeto auditable:

- Verificación de controles generales de TI, que conllevaría el análisis de determinados controles asociados a la protección de la información tanto física como lógica.
- De cumplimiento de normativa y/o legislación aplicable.
- Seguridad física: en relación a la verificación de los sistemas medioambientales que protegen los sistemas informáticos.
- Seguridad lógica: en relación a la verificación de los sistemas de identificación, control de acceso para proteger la información residente en los sistemas de información
- Calidad
- Operativa / Procesos
- Gestión eficiencia / eficacia
- Investigación delitos y/o fraude
- Apoyo a otras auditorías: auditoría de cuentas, auditorías fiscales, etc. teniendo en cuenta que los procesos informáticos dan soporte a la operativa a auditar.

5.5 Desarrollo Auditoría

La Auditoria consta de varias fases, en este apartado se va a describir cada una de ellas indicando las actividades principales asociadas.

Una auditoría se llevará a cabo:

- Cuando sea necesario proceder a una evaluación independiente y sistemática.
- Cuando sea necesario determinar la eficacia de los procedimientos llevados a cabo.
- Cuando se efectúen modificaciones en la organización que puedan afectar al correcto funcionamiento de la misma.

5.5.1 Planificación y preparación

La primera fase viene determinada por establecer el ámbito y alcance de la auditoría así como el equipo de trabajo que va a llevarla a cabo. Dentro de esta fase se encuentran las siguientes subfases:

1. *Elaboración del plan de Auditoría*

   Tanto la organización como la auditora prepararán un documento donde se indiquen de forma explícita los principios y procedimientos detallados para la organización de la auditoría, en este documento se deben incluir:

   - Declaración relativa a la responsabilidad, independencia y autoridad de los auditores.
   - Medidas para la contratación de especialistas en casos puntuales.
   - Medidas para el acceso del equipo auditor a las instalaciones, documentos cuando sea necesario para el desarrollo de la auditoría.

   Se prepara un programa de trabajo donde se describa la auditoría, junto con los correspondientes documentos (tareas a realizar, detalle de documentos a revisar, relación de entrevistas, etc.)

   En el programa de trabajo se debe indicar:

   - Objeto y alcance de dicho programa de trabajo.
   - Requisitos de la Auditoría
   - Equipo de trabajo encargado de realizar la auditoría
   - Tareas/actividades comprendidas en la auditoría.

2. *Organización del equipo de Auditoría*

   Las personas que compongan el equipo de trabajo deberán tener conocimientos y experiencia profesional del programa de trabajo que vayan a auditar.

   Se elegirá un jefe de equipo que se encargará de:

   - Gestión y coordinación del equipo de auditoría
   - Participación en el desarrollo de la auditoría
   - Publicación del informe
   - Coordinación de actividades de auditoría

   La entidad auditada pondrá a disposición del equipo de auditoría toda la información necesaria así como los procedimientos, normas, instrucciones, códigos e informes de anteriores auditorías.

3. Notificación de la Auditoria

La entidad a auditar deberá recibir notificación previa de la auditoría, en esta notificación se deberá incluir:

- Objeto y alcance
- Programa de la auditoría
- Componentes del equipo auditor

Adicionalmente el equipo auditor deberá recibir:

- Acuse de recibo de la notificación
- Nombre de las personas responsables o encargadas de las actividades o áreas a auditar.

5.5.2 Realización

Comprende tres fases:

1. Reunión previa

Al inicio de la auditoría se mantendrá una reunión con la finalidad de:

- Confirmar el objeto y alcance de la auditoría
- Confirmar las fechas propuestas para el desarrollo de la misma.
- Presentar los componentes del equipo de auditoría al personal de la entidad auditada.
- Establecer los canales de comunicación
- Establecer la planificación y cierre de la auditoría

2. Desarrollo de la auditoría

El desarrollo de la auditoría se realizará conforme al programa de trabajo

Cualquier no conformidad se identificará y se trasladará con la mayor exactitud posible, a fin de determinar las causas que la originan y el efecto que pueda producirse, comunicando a la dirección de la entidad auditada la no conformidad para que ésta pueda adoptar las medidas oportunas para la subsanación de la misma cuanto antes.

3. Reunión final de auditoría

Una vez finalizada la auditoría, se mantendrá una reunión con los responsables de la entidad auditada con el fin de informar sobre las no conformidades encontradas y aclarar las dudas que hayan podido surgir en el desarrollo de la misma.

Las no conformidades se incluirán en el informe de auditoría que será firmado por el jefe de equipo de auditoría y por el responsable de la entidad auditada.

5.5.3 Elaboración del Informe de Auditoría

El equipo de auditoría preparará el informe, éste contendrá los siguientes apartados:

- Descripción del objeto y alcance de la auditoría
- Listado de los miembros del equipo auditor
- Listado de las personas que hayan sido entrevistadas
- Breve resumen de las áreas objeto de la auditoría
- Lista detallada de las conclusiones a las que se ha llegado una vez finalizado la auditoría
- Detalle del hecho observado, en este apartado se incluirá el detalle de la incidencia detectada.
- Descripción de la incidencia, donde se hará referencia a la normativa infringida.
- Detalle de la recomendación a llevar a cabo para la subsanación de la incidencia.

5.5.4 Seguimiento

El seguimiento de las recomendaciones posteriores a la Auditoría tiene por objeto comprobar que se llevan a cabo las acciones correctoras derivadas de las no conformidades detectadas.

Este seguimiento lo podrán llevar a cabo tanto la entidad auditada como el equipo auditor.

Capítulo 6

Auditoría de las medidas de seguridad establecidas en el Título VIII del RLOPD

6.1 Auditoría Reglamento

Este capítulo describe un modelo de programa de trabajo y las correspondientes pruebas de auditoría a realizar por el equipo de auditoría con el fin de realizar la Auditoría bienal requerida por el Reglamento de Desarrollo de la LOPD.

El objetivo, por tanto es verificar el grado de cumplimiento con las medidas de Seguridad establecidas por el Reglamento de Desarrollo de la LOPD en su Título VIII.

El primer aspecto que es necesario tener en cuenta es la distinción entre el cumplimiento de las medidas de seguridad en ficheros automatizados o no automatizados, para ello, se ha dividido en estos dos grandes epígrafes, a su vez estos dos apartados se desglosan en los niveles de seguridad aplicables.

A continuación, se va a describir cada uno de los capítulos que componen el Título VIII y para cada artículo descrito en la normativa:

- Interpretación del mismo en un lenguaje técnico.
- Relación de pruebas de auditoría que sería necesario llevar a cabo.
- Evidencias a solicitar.
- Valoración de qué aspectos se tendrían que tener en cuenta para valorar el cumplimiento o no de la medida de seguridad.

6.2 Capítulo I. Disposiciones generales

Dentro de este capítulo se incluyen, tal y como indica el nombre medidas de seguridad relacionados con aspectos generales.

6.2.1 Artículo 79. Alcance

[Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento]

En cumplimiento de este artículo se especifica que los responsables de la implantación de las medidas de seguridad serán tanto responsables de ficheros como encargados del tratamiento.

De esta forma, una Entidad que disponga sus sistemas de información externalizados en otra, tendrá responsabilidad de determinadas medidas exigidas en el Reglamento y por su parte, la entidad encargada de la prestación del servicio informático también será responsable de la implantación de medidas de seguridad.

6.2.2 Artículo 80. Niveles de seguridad

[Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.]

En este artículo se describen los 3 posibles niveles en los que estará clasificada la información que contenga datos de carácter personal.

6.2.3 Artículo 81. Aplicación de los niveles de seguridad

[1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.
2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los relativos a la comisión de infracciones administrativas o penales.

b. Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c. Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d. Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e. Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f. Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a. Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b. Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c. Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b. Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.]

En este artículo se explican los distintos niveles de seguridad que se definen en el Reglamento, y que será de vital importancia para determinar qué medidas de seguridad son aplicables en cumplimiento de la normativa.

De esta forma es vital conocer, que cualquier fichero y/o aplicación que contenga datos de carácter personal será necesario dotarle de medidas de seguridad al menos de nivel básico.

Las medidas de seguridad serán acumulativas, en función de la clasificación establecida, será necesario adoptar medidas superiores, siendo requerida la implantación de medidas de nivel medio (además de las de nivel básico) o alto (además de las de nivel medio y nivel básico).

6.2.4 Artículo 82. Encargado del tratamiento

[1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.
2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.
3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.]

En este artículo se hace referencia a dos posibles escenarios que se pueden tener en relación a los encargados del tratamiento:

- El primer caso, está referido a responsables del fichero que facilitan el acceso al encargado en sus propios locales.

  Este caso sería, por ejemplo, cuando se dispone de personal externo que accede a la información a través de los recursos del responsable (se le proporciona acceso a los sistemas, equipos informáticos..), el proveedor se encuentra en las propias instalaciones del responsable y la prestación que realiza es directamente a través de aplicaciones/ sistemas de información del responsable.

  Se contempla también la posibilidad de que el acceso a la información sea vía remota, en estos casos se el acceso debería ser a través de puestos/ sesiones virtuales que impidan técnicamente que el proveedor pueda extraer información fuera de los recursos propios del responsable.

- El segundo caso, se refiere a cuando el responsable facilita datos al encargado para que éste en sus instalaciones y/o recursos propios realice la prestación del servicio solicitada.

  Este caso sería, por ejemplo, una imprenta, a la que el responsable del fichero facilita una base de datos de los empleados para la impresión de las tarjetas de visita

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 82.1:	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los locales del responsable del fichero, se incluye esta información en el documento de seguridad.

La compañía debe disponer de un listado con todas las subcontrataciones que se dispongan y del tipo de acceso a la información de la compañía/ tratamiento que pueda existir, de esta forma en el inventario se tiene que disponer de:

- Subcontrataciones que no impliquen acceso ni tratamiento de datos de carácter personal.
- Subcontrataciones que impliquen un acceso a información de la compañía a través de sistemas propios de la compañía.
- Subcontrataciones que impliquen la entrega de determinada información y por tanto, una salida de información de la compañía hacia las instalaciones del proveedor.

La primera acción a realizar sería identificar qué posibles subcontrataciones puede existir en la compañía que conlleven un tratamiento de datos de carácter personal en las instalaciones de la compañía, pueden ser por ejemplo:

- Personal subcontratado que accede a los sistemas de la compañía y que está físicamente instalado en las instalaciones de ésta, puede ser dentro de cualquier área como personal externo.
- Personal informático: desarrolladores, personal de mantenimiento de sistemas, infraestructuras.

Prueba 82.2:	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los locales del responsable del fichero, existe un contrato/compromiso de confidencialidad firmado por parte del personal del encargado del tratamiento en cumplimiento de las medidas de seguridad.

Se recomienda incluir un documento en el que el personal reciba las normas y procedimientos que debe cumplir.

Dentro de las medidas que tendría que incluirse se encuentran:

- Medidas de seguridad física: los contratos de encargo del tratamiento deben de disponer de cláusulas específicas acerca de:
    - No obtención de datos de carácter personal, ni extracción, ni reproducción de los mismos fuera de las instalaciones de la compañía.
    - No realizar salida de información de ningún tipo de las instalaciones de la compañía.

    - Deber de secreto respecto de las normas de seguridad de aplicación.

- Concienciación al personal de la compañía en relación a espacio de trabajo recogido.
  Se deben establecer también aspectos de concienciación a los propios empleados de forma que no dejen información sin vigilar en mesas, fotocopiadoras e impresoras, que puedan ser accedidas por personal no autorizado.

- Medidas de seguridad lógica.
  Establecer medidas de seguridad lógica de para controlar el acceso a los sistemas de información y existencia de perfiles que permitan delimitar las funcionalidades acorde a las funciones y responsabilidades del personal.

  Adicionalmente, se deben valorar las medidas adoptadas para la protección de la información y evitar en la medida de lo posible las fugas de información, de esta forma se recomienda establecer diferentes medidas como pueden ser:

    - Establecer puestos virtuales para el control del acceso a la información.
    - Bloqueo puertos USB que impidan el uso de estos dispositivos.
    - No permitir la impresión de listados con información de la entidad.
    - No permitir la salida de información vía correo electrónico a direcciones de correo de fuera de la entidad.

Prueba 82.3:	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los propios locales del encargado del tratamiento, se incluye esta información en el documento de seguridad.

El listado descrito en los apartados anteriores debe constar en el Documento de Seguridad de la compañía o bien redireccionar a donde se encuentre el mismo. Se deberá incluir:

- En qué consiste la prestación y su vigencia.
- Sobre qué ficheros declarados a la AEPD se presta el servicio.
- El nivel de los datos tratados y que será por tanto exigido en el contrato de prestación de servicios entre Responsable del Fichero y Encargado del Tratamiento.

Prueba 82.4:	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los propios locales del encargado del tratamiento, existe un contrato/compromiso de confidencialidad firmado por parte del personal del encargado del tratamiento en cumplimiento de las medidas de seguridad.

Dentro de las medidas que tendría que incluirse en el contrato entre ambas partes se encuentran:

- Medidas de seguridad:
    - Obligación por parte del encargado de la implementación de las medidas de seguridad acorde con el nivel de los datos.

- Devolución y/o destrucción segura de la información del responsable.
- No llevar a cabo ninguna subcontratación por parte sin la autorización de la compañía (responsable).
- Deber de secreto respecto de la información.

- Concienciación al personal de la compañía en relación a espacio de trabajo recogido.
  Se deben establecer también aspectos de concienciación a los propios empleados de la empresa del proveedor.

- Valorar medidas de enmascaramiento/disociación de datos
  Se deben valorar aspectos relativos a no proporcionar datos de carácter personal al proveedor, salvo los casos en los que sea estrictamente necesario.

  De esta forma, se tendría que tener en cuenta si se pueden aplicar procedimientos de enmascaramiento o disociación de datos de forma que no se realicen entregas de datos a prestadores de servicios y por tanto, minimizar el riesgo de fuga de información confidencial de la Entidad.

Prueba 82.5:	Verificar la existencia de un documento de seguridad del encargado del tratamiento que verifique que éste posee identificado el fichero y que implementa las medidas de seguridad requeridas.

Es necesario verificar que el encargado del tratamiento disponga de un documento de seguridad relativo al tratamiento llevado a cabo.

De esta forma, el encargado podrá haberlo incluido en su propio documento de seguridad o llevar a cabo uno específico para el servicio prestado.

Prueba 82.6:	Verificar la existencia de un documento en el que se establezca el compromiso por parte del encargado del tratamiento para la implantación de las medidas de seguridad

En cualquiera de los casos, este el encargado en las instalaciones del responsable o en sus propias instalaciones hay que tener en cuenta que deben cumplirse las medidas de Seguridad.

Para ello, es necesario que el encargado proporcione al responsable alguna carta/documento que acredite el compromiso por su parte en el cumplimiento de estas medidas, este documento podría proporcionarse anualmente.

6.2.5 Artículo 83. Prestaciones de servicios sin acceso a datos personales

[El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.]

En este caso, el Reglamento considera los proveedores que realizan una prestación de servicio que no conlleva en sí un acceso y/o tratamiento de datos de carácter personal. Dentro de esta prestación se encontraría, por ejemplo, personal de limpieza, jardinería, consultoría de análisis de mercados o servicios que no necesitarán datos e información del responsable de ficheros para realizar el trabajo.

En estos casos, la responsabilidad del responsable del fichero viene encaminada a evitar que estos proveedores puedan llegar a acceder a información/sistemas del responsable.

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 83.1:	Verificar qué medidas se han adoptado para impedir el acceso a los datos en encargos en que no hay datos de carácter personal

La primera acción a realizar sería identificar qué posibles subcontrataciones puede existir en la compañía y que no conlleven un tratamiento de datos de carácter.

Dentro de las medidas que habría que revisar se encuentran:

- Concienciación al personal de la compañía en relación a espacio de trabajo recogido.
  Se deben establecer también aspectos de concienciación a los propios empleados de forma que no dejen información sin vigilar en mesas, fotocopiadoras e impresoras, que puedan ser accedidas por personal no autorizado.

- Archivo de la Documentación
  Se debe revisar dónde se archiva la documentación, de forma que no sea sencillo su acceso por personal no autorizado.

  Por ejemplo, es recomendable el uso de impresoras seguras, de forma que la información únicamente es impresa en papel cuando el usuario introduce su tarjeta acreditativa, protegiendo de este modo la confidencialidad de la información.

  De igual forma, los faxes/ correo interno deberían estar situados en zonas protegidas cuyo acceso estuviera controlado.

- Medidas de seguridad lógica.
  Establecer medidas tales como utilización de protectores de pantalla con contraseña, contraseñas de acceso a los sistemas de información que imposibiliten el acceso a personal no autorizado.

Prueba 83.2:	Verificar la existencia de un contrato en el que se recoja expresamente la prohibición de acceder a datos personales y el secreto profesional de la información que pudieran llegar a conocer con motivo de la prestación del servicio.

Es necesario revisar que, en este tipo de contratos de encargo del tratamiento se disponga de cláusulas específicas acerca de la no obtención de datos de carácter personal, ni reproducción de los mismos.

Dado que, si bien el tratamiento no conlleva acceso ni tratamiento de datos, pueden acceder de forma colateral a la información, habrá que incluir cláusulas específicas acerca de:

- No obtención de datos de carácter personal, ni extracción, ni reproducción de los mismos (Información que pueda existir por ejemplo sobre las mesas, en las fotocopiadores, armarios..)
- No realizar salida de información de ningún tipo de las instalaciones de la compañía.
- Deber de secreto de cualquier aspecto que pueda conocer derivado del servicio prestado.

6.2.6 Artículo 84. Delegación de autorizaciones

[Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 84.1:	Verificar que en el Documento de Seguridad consta una referencia del responsable autorizado para delegar las diferentes responsabilidades.

Verificar que se dispone de la correspondiente autorización (si aplica) en el Documento de Seguridad.

Prueba 84.2:	Verificar que en el Documento de Seguridad consta una referencia a las personas designadas como responsables por delegación del responsable del fichero.

Verificar que, si existen delegaciones, se encuentran documentadas en el Documento de Seguridad.

6.2.7 Artículo 85. Acceso a datos a través de redes de comunicaciones

[Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 85.1:	Verificar la infraestructura de redes de comunicaciones con el fin de identificar si las medidas de seguridad corresponden con las medidas implantadas en modo local.

6.2.8 Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento

[1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 86.1:	Determinar la existencia de ordenadores portátiles

Si la compañía dispone de ordenadores portátiles, será un medio de realizar tratamiento de los datos fuera de las instalaciones, por ello, será necesario garantizar qué medidas específicas existen en relación a la autorización y las medidas de seguridad aplicables a éstos dispositivos, en concreto:

- Verificar que existe un procedimiento establecido para la gestión y autorización del equipo, que incluya solicitud del equipo, autorización, y una gestión de la entrega de dicho equipo al usuario que vaya a responsabilizarse del mismo.

  Los ordenadores portátiles habitualmente están gestionados por el centro de atención de usuarios dentro del área de Informática. Para ello, será necesario revisar todo el proceso de gestión que se sigue para la asignación:

  - Herramienta informática que mantenga tener identificado a quién pertenece el ordenador portátil y el período de asignación del mismo (indefinido, asignado por tiempo necesario para llevar a cabo un determinado proceso, etc…

  - Teniendo en cuenta que esta herramienta también tendrá que estar identificada en la sección de Estructura de ficheros de datos de carácter personal en el Documento de Seguridad de la compañía.

  - Inventario de los ordenadores portátiles. Pudiendo obtenerse de la herramienta un listado de los mismos.

  - Relación de software /BBDD que puede contener el portátil.

  - Es recomendable disponer de esta información por varios motivos: a nivel operativa, para conocer cómo se ha plataformado el equipo, y por motivos de seguridad, ante pérdida o robo del equipo podemos conocer qué tipo de información se encuentra expuesta a accesos no autorizados.

  - Existencia de herramientas de cifrado.
    Si bien, solo está exigido por el Reglamento en las medidas de nivel alto, es posible que, la compañía desee implantar estas medidas para proteger la confidencialidad de la información independientemente del nivel de seguridad LOPD asociado. Esto es especialmente importante en casos de pérdida o robo del portátil ya que no se comprometería la información que pudiera contener.

    De esta forma existen áreas más críticas dentro de las compañías en las que puede ser recomendable esta medida: Áreas de Dirección, RRHH, Auditoría Interna, e incluso aunque éstos dispositivos no fueran a salir de las instalaciones.

  - Es recomendable asignar junto al ordenador portátil de un cable de seguridad que permita el anclaje del dispositivo, de esta forma podemos evitar robos de los mismos, lo que conlleva pérdidas económicas y riesgo de acceso no autorizado a la información que pudiera contener el portátil.

  - De igual forma, existen en el mercado unas láminas denominadas “Filtros de privacidad” que se colocan sobre la pantalla del ordenador portátil y que solo permiten la visión a la persona que se encuentra delante del mismo impidiendo la visión desde cualquier otro ángulo.

- Verificar que se informa del cumplimiento de las medidas de seguridad en función del tratamiento de los datos: notas específicas, documento firmado de "Recibí el equipo" en el que se indiquen las medidas de seguridad a aplicar.

  El usuario debe conocer las medidas de seguridad que debe cumplir en relación a estos dispositivos, por lo que se recomienda que exista un documento de conformidad, en el que se indique al usuario aspectos tales como:

  - Responsabilidad el usuario sobre el equipo.
  - Implicaciones que tiene la pérdida del equipo sobre la información que contenga el mismo.

Prueba 86.2:	Determinar la existencia de dispositivos de almacenamiento externo

En la actualidad las compañías utilizan de forma habitual pen-drives o soportes que puedan contener información con datos de carácter personal, éstos son especialmente sensibles por la facilidad que permiten para el intercambio de la información, para la sustracción o pérdida de los mismos, y por tanto, el acceso no autorizado a la información, para verificar el estado de la compañía en relación a este tema considero necesario:

- Verificar que existe un procedimiento establecido para la gestión y autorización del dispositivo, de igual forma que para los equipos, este procedimiento debe contemplar solicitud del dispositivo, autorización, y una gestión de la entrega de dicho dispositivo al usuario que vaya a responsabilizarse del mismo.

  Los dispositivos portátiles también suelen estar gestionados por el centro de atención de usuarios dentro del área de Informática. Para ello, será necesario revisar todo el proceso de gestión que se sigue para la asignación:

  - Herramienta informática con la relación de dispositivos externos existentes en la compañía y su asignación.
  - Tener en cuenta que esta herramienta también tendrá que estar identificada en la sección de Estructura de ficheros de datos de carácter personal en el Documento de Seguridad de la compañía.
  - Utilización de mecanismos de cifrado de los dispositivos.
  - Custodia de los dispositivos.
  - Destrucción segura de la información contenida en los mismos.
  - Medidas de seguridad a llevar a cabo ante la reutilización de los dispositivos.

- Verificar que se informa del cumplimiento de las medidas de seguridad en función del tratamiento de los datos: notas específicas, documento firmado de "Recibí el dispositivo" en el que se indiquen las medidas de seguridad aplicar.

  El usuario debe conocer las medidas de seguridad que debe cumplir en relación a estos dispositivos, por lo que se recomienda que exista un documento de conformidad, en el que se indique al usuario aspectos tales como:

- Responsabilidad del usuario sobre el dispositivo y sobre la información contenida en el mismo.
- Implicaciones que tiene el intercambio de información con personal no autorizado a acceder a la información contenida en el dispositivo.
- Implicaciones que tiene la pérdida del equipo sobre la información que contenga el mismo.

Prueba 86.3:	Determinar existencia de otros dispositivos que puedan contener datos

Si la Entidad dispone de otros dispositivos portátiles tales como smartphones, tablets, será necesario garantizar que existen medidas en relación a la autorización y las medidas de seguridad aplicables, en concreto:

- Verificar que existe un procedimiento establecido para la gestión y autorización de este tipo de dispositivos, de igual forma que para los equipos, este procedimiento debe contemplar solicitud del dispositivo, autorización, y una gestión de la entrega de dicho dispositivo al usuario que vaya a responsabilizarse del mismo.

- Verificar que se informa del cumplimiento de las medidas de seguridad en función del tratamiento de los datos: notas específicas, documento firmado de "Recibí el dispositivo" en el que se indiquen las medidas de seguridad a aplicar.

- Es necesario conocer la Política de movilidad que disponga la compañía, para conocer si pueden existir otros dispositivos de este tipo que puedan estar siendo utilizados y que puedan conllevar un tratamiento fuera de los locales.

Prueba 86.4:	Verificar que en el Documento de Seguridad se incluyen referencias a las autorizaciones para el uso de portátiles u otros dispositivos de almacenamiento de datos

Dicha autorización, deberá contener:

- Usuario / grupo de usuarios autorizados.
- Vigencia de la autorización.

6.2.9 Artículo 87. Ficheros temporales o copias de trabajo de documentos

[1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 87.1:	Verificar las medidas que se han adoptado sobre los ficheros temporales o copias de documentos

- Archivos temporales de procesos de aplicaciones.
- Archivos generados por el usuario.

Dichos ficheros deberán contemplar las medidas de seguridad correspondientes al nivel del mismo.

Prueba 87.2:	Verificar las medidas que se han adoptado sobre los ficheros temporales o copias de documentos cuando éstos hayan dejado de existir

- Archivos temporales de procesos de aplicaciones.
- Archivos generados por el usuario.

  Dichos ficheros deberán ser eliminados cuando ya no sean necesarios.

6.3 Capítulo II. Del Documento de Seguridad

6.3.1 Artículo 88. El documento de seguridad

[1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:
a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:
a) La identificación del responsable o responsables de seguridad.
b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad.

Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.
En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 88.1:	Verificar la existencia de un Documento de Seguridad.

Es necesario verificar que exista un Documento de Seguridad que recoja los aspectos requeridos por el Reglamento de Desarrollo de la LOPD, para ello, es necesario tener en cuenta que pueden existir uno o varios, en función de cómo se haya organizado en la Entidad correspondiente.

Prueba 88.2:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto el Documento debe contener:
- Ámbito de aplicación del Documento.

Prueba 88.3:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:

- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.

Prueba 88.4:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:

- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

En el siguiente apartado se indicarán algunos de los grupos de usuarios a modo de ejemplo que se deberían tener en cuenta: programadores, administradores, usuarios..

Prueba 88.5:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:

- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

En este sentido, se recomienda incluir la siguiente información:

- Nombre del Fichero Lógico, tal y como está declarado en el RGPD.

- Responsable de Seguridad, quién ejercita las labores de Responsable de Seguridad establecidas para este fichero lógico.

- Nivel de Seguridad, indica el nivel de medidas de seguridad (básico, medio o alto) que debe cumplir el fichero en función de los datos que contiene.

- Finalidad, indica la finalidad de los datos de carácter personal que forman el fichero lógico.

- Descripción, para describir de forma general el carácter de la información contenida en el fichero lógico.

- Sistema de tratamiento, entendiendo como tal el modo en que se organiza o utiliza un sistema de información.
- Tipo de sistema de información, pudiendo ser automatizados, no automatizados o parcialmente automatizados.

- Sistema operativo, indica el nombre y versión del sistema operativo sobre el que se encuentran instaladas las bases de datos y aplicaciones que contienen los datos de carácter personal.

- Base de datos, indica el nombre y versión del sistema de gestión de base de datos (o sistema de ficheros si procede) que almacenan los datos de carácter personal y que sirven de soporte a las aplicaciones.

- Aplicación, indica el nombre y versión de las aplicaciones que tratan los datos de carácter personal.

- Nombre del servidor, indica el nombre del servidor o servidores en que residen los datos de carácter personal.

- Ubicación física, indica el lugar físico en el que residen los datos de carácter personal.

Prueba 88.6:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:
- Procedimiento de notificación, gestión y respuesta ante las incidencias.

Prueba 88.7:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

Prueba 88.8:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:
- Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Prueba 88.9:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:
- La identificación del responsable o responsables de seguridad.

Prueba 88.10:	Revisar si el Documento de Seguridad contiene cada uno de los aspectos requeridos.

En concreto, el Documento de Seguridad debe contener:

- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

Prueba 88.11:	Verificar (si existe) para cada tratamiento de datos por cuenta de terceros, determinada información en el Documento de seguridad

En concreto, habrá que verificar:

- Identificación de ficheros o tratamientos.
- Referencia al contrato o documento que regule.
- Identificación del responsable.
- Vigencia del encargo.

Prueba 88.12:	Verificar que, en los contratos con Proveedores en los que se van a realizar tratamientos de datos en las instalaciones del Proveedor se ha incluido la obligatoriedad de que el Proveedor anote estos temas en su documento de Seguridad

Verificar que existe esta referencia en los contratos con los proveedores cuyo acceso a la información de la entidad se realice en las propias instalaciones del proveedor.

Prueba 88.13:	Verificar si el Documento de Seguridad se encuentra actualizado; verificar los procedimientos descritos en el Documento de seguridad vs Procedimientos reales implantados.

Verificar si el documento se encuentra actualizado, para ello:

- Comprobar que la información que se detalla en los procedimientos y documento de seguridad se encuentra debidamente implantada en las áreas correspondientes de la entidad.

Prueba 88.14:	Comprobar si el Documento de Seguridad posee un control de versiones que asegure que éste se revisa periódicamente realizando las modificaciones pertinentes

Verificar si el documento se encuentra actualizado, para ello:

- Verificar que se dispone de un adecuado control de versiones.
- Verificar que el documento de seguridad y procedimientos asociados recogen modificaciones importantes en la entidad y en los sistemas de información afectados.

Prueba 88.15:	Comprobar durante la revisión del Documento de Seguridad que éste se adecua a todas las disposiciones vigentes en materia de seguridad.

Verificar que el documento de seguridad recoge en su ámbito de aplicación todas las disposiciones vigentes en materia de Seguridad.

6.4 Capítulo III. Medidas de Seguridad aplicables a ficheros y tratamientos automatizados

6.4.1 Sección I. Medidas de seguridad de nivel básico

6.4.1.1 Artículo 89. Funciones y obligaciones del personal

[1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 89.1:	Verificar que se ha descrito en el Documento de Seguridad o Documento anexo que refleje las funciones y obligaciones del personal que tiene acceso a datos de carácter personal.

Este documento debería tener la definición de distintos grupos y/o colectivos que pueden tener acceso a la información, por ejemplo:

- Responsable del Fichero
  El responsable del fichero es la persona física o jurídica propietaria de los datos, que decide sobre la finalidad, contenido y uso del tratamiento de los ficheros con datos de carácter personal.

- Responsable del Tratamiento

La figura del responsable del tratamiento garantiza a la Entidad que el referido tratamiento se realiza con las debidas garantías de confidencialidad, de acuerdo a las instrucciones recibidas y aplicando las medidas de seguridad que, en virtud de la naturaleza de los datos tratados, sean legalmente exigibles.

- Responsable de Seguridad
  Funciones básicas:

  - Coordinar y controlar las medidas definidas en el Documento de Seguridad en virtud de lo dispuesto en la normativa vigente sobre protección de datos de carácter personal.
  - Asegurar las actividades de concienciación y formación en aspectos relativos a la seguridad de la información a nivel local.
  - Actualizar el Documento de Seguridad cuando sea necesario, debido a modificaciones en la operativa de la Entidad en materia de protección de datos

- Usuarios.
  Entendemos por usuario a cualquier persona autorizada que tiene acceso a los datos de carácter personal.

  En particular, deberán cumplir con los procedimientos definidos en el Documento de Seguridad, solicitando autorización para las acciones que así lo requieran según se establece por los canales habilitados. Concretamente deben prestar atención a:

  - Confidencialidad respecto de la información y documentación que reciben o usan por motivo de sus funciones.
  - No incorporar a la entidad información o datos obtenidos sin la autorización de la entidad.
  - En especial, no ceder datos de carácter personal ni usarlos con finalidad distinta a la del fichero al que se hallen incorporados.
  - Mantener secreto respecto a contraseñas y claves de acceso.
  - Comunicar al Responsable de Seguridad cualquier incidencia respecto a la seguridad de los datos de carácter personal o de las medidas de seguridad conforme al procedimiento existente de gestión de incidencias.

- Responsable de Aplicación
  Las funciones de los Responsables de las aplicaciones consisten en asegurar el cumplimiento de las medidas de seguridad según el nivel de la aplicación así como velar por el cumplimiento de los procedimientos asociados a la gestión de usuarios.

- Programadores.
  Desarrollo y mantenimiento de la aplicación, solución de incidencias y actualización de versiones. Deben acceder únicamente a entornos de desarrollo y pruebas donde los datos estén disociados o no haya datos reales.

- Administradores.
  Personal autorizado para llevar a cabo la administración de los sistemas asignados.

  Mantenimiento de la aplicación, solución de incidencias y actualización de versiones.

Deben acceder a los datos únicamente para el desarrollo de las funciones anteriormente indicadas, sin posibilidad de realizar extracciones de datos salvo autorización expresa de la entidad.

Prueba 89.2:	Verificar si existen funciones delegadas por el responsable del fichero, que se encuentran documentadas en el Documento de Seguridad o documentación anexada a éste

Es posible que se dispongan de determinadas funciones delegadas en:
- usuarios administradores
- usuarios autorizadores
- ..

En éstos casos deberán constar en el Documento de Seguridad o en algún anexo que esté referenciado.

Prueba 89.3:	Verificar los mecanismos empleados por el responsable del fichero/tratamiento para que el personal conozca las normas de seguridad.

La información que se debería dar a conocer incluye:

- Información relativa al Reglamento y leyes en cumplimiento de la LOPD.
- Documento de Seguridad, procedimientos de seguridad o información concreta que incluya las medidas de seguridad que afecten a la utilización de datos de carácter personal por parte de los distintos usuarios de la Entidad.

A modo de ejemplo las posibles vías podrían ser:

- Intranet, mostrando información relativa al Reglamento, Documento de Seguridad o extracto de éste que incluya las medidas de seguridad más relevantes.
- Envío de correos electrónicos informativos periódicos.
- Cursos de formación, etc.

6.4.1.2 Artículo 90. Registro de incidencias

[Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 90.1:	Verificar que existe un procedimiento de notificación y gestión de incidencias que afecten a los datos de carácter personal.

Este procedimiento debe contener:

- Cómo se gestionan las incidencias, desde su reporte inicial por parte de los usuarios que detectan una incidencia.
- A qué áreas o grupos de trabajo es necesario que los usuarios reporten las incidencias.
- Cómo se gestionan dichas incidencias, herramientas utilizadas para su gestión, resolución y correspondiente cierre.

Prueba 90.2:	Verificar que existe un registro de incidencias.

Dentro de los aspectos que será necesario tener en cuenta para la gestión de las incidencias se incluye un registro en el que se archiven todas las incidencias que afecten a los datos de carácter personal.

Prueba 90.3:	Verificar que el Registro de Incidencias contiene el tipo de incidencia

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya el Tipo de incidencia. Una incidencia se define como cualquier anomalía que puede afectar a la seguridad de los datos, de esta forma pueden existir incidencias:

- Accesos no autorizados a salas de acceso restringido donde residan sistemas de información automatizados o no que contengan datos de carácter personal.
- Robos de documentación, pérdidas de dispositivos que contengan información con datos de carácter personal.
- Acceso no autorizado a los sistemas de información.
- Bloqueo tras superar un número de intentos fallidos.
- Fallo en la realización de los procedimientos de realización de copias de respaldo.
- ..

Prueba 90.4:	Verificar que el Registro de Incidencias contiene el momento en que se ha producido la incidencia o detectado.

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya el momento en que se ha producido la incidencia o detectado la incidencia.

Para ello será necesario incluir la fecha y la hora en que se ha producido o detectado la incidencia.

Prueba 90.5:	Verificar que el Registro de Incidencias contiene la persona que realiza la notificación

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya el nombre de la persona que realiza la notificación.

Prueba 90.6:	Verificar que el Registro de Incidencias contiene a quién se comunica la incidencia

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya a quién se comunica la incidencia.

Prueba 90.7:	Verificar que el Registro de Incidencias contiene los efectos que se hubieran derivado de la incidencia

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya los efectos derivados de las incidencia, para ello deberá constar la información acerca de la descripción de la incidencias, del hecho producido y qué problemas se han derivado de la misma.

Prueba 90.8:	Verificar que el Registro de Incidencias contiene las medidas correctoras aplicadas

El Registro de incidencias indicado en la prueba 90.2 deberá contener un campo que incluya las medidas correctoras aplicadas, para ello, se deberá incluir información acerca de las medidas que se han adoptado, procedimientos llevados a cabo u otros aspectos que se hayan llevado a cabo con el fin de mitigar la incidencia.

6.4.1.3 Artículo 91. Control de acceso

[1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 91.1:	Verificar los accesos permitidos a los usuarios

Para ello identificar grupos de trabajo/Departamentos y verificar que realmente son los usuarios que deberían tener dicho acceso.

Prueba 91.2:	Verificar que existen mecanismos para obtener una relación actualizada de los usuarios y perfiles de usuario.

Revisar los procedimientos existen para comprobar que el listado esté actualizado, verificar los canales para la comunicación de bajas de empleados, obteniendo información acerca de los usuarios dados de baja de la Empresa y que poseen un usuario activo en los sistemas, y/o revisión de los procedimientos existentes en relación a cambios de departamentos y/o funciones asignados a los empleados de la Entidad.

Prueba 91.3:	Verificar que los sistemas de información disponen de mecanismos de protección para limitar el acceso.

Por ejemplo:

- Identificador y contraseña para restringir los accesos.
- Grupos de usuarios con perfiles delimitados.
- Limitaciones en la utilización de los usuarios administradores.

Prueba 91.4:	Verificar que existen procedimientos de revisión por parte de la Entidad para verificar periódicamente que los usuarios disponen del acceso necesario para el desarrollo de sus funciones.

Para valorar esta prueba será necesario revisar qué acciones se realizan respecto a revisiones de usuarios:

- Informes periódicos de cada departamento con los perfiles y funciones asignadas.
- Procedimiento de bajas de usuarios: existencia de una comunicación desde áreas de RRHH a las áreas de gestión de usuarios para detectar bajas de usuarios y proceder a su bloqueo.
- Existencia de medidas técnicas que bloqueen el usuario tras superado el límite de inactividad, de forma, que se puedan detectar accesos que ya no son necesarios para el usuario.

Prueba 91.5:	Verificar que en el Documento de Seguridad aparece un listado o se referencia al listado de personal de administración encargado de conceder, alterar o anular el acceso autorizado a los recursos.

En el documento de Seguridad deberá aparecer qué áreas son las que participan en los procesos de gestión de usuarios: encargadas de la gestión de usuarios y áreas encargadas de la autorización.

Prueba 91.6:	Verificar que el personal externo se incluye dentro de las mismas políticas de Seguridad:

En el documento de Seguridad deberá aparecer la política, que deberá ser la misma para el personal externo, será necesario verificar por tanto que existe:

- Validación usuario/contraseña.
- Mecanismos de acceso físico.

6.4.1.4 Artículo 92. Gestión de soportes y documentos

[1. Los soportes que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.

3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 92.1:	Verificar que los soportes están etiquetados de forma que es posible identificar la información que contienen

Esto será posible, a través de una etiqueta con información comprensible o a través de un código de barras del que pueda obtenerse la información a través de una herramienta automatizada de gestión de soportes.

Prueba 92.2:	Verificar que existe un inventario con los soportes de la Entidad.

Para ello, es necesario verificar la existencia de distintas opciones:

- un inventario físico
- una herramienta automatizada que permita obtener la información acerca de los soportes que disponga la Entidad.
- Robot, que permite la custodia e inventario de los soportes.

Prueba 92.3:	Verificar que en el Documento de Seguridad se establece quién puede acceder a los soportes

Para ello, es necesario definir en el Documento de Seguridad, qué áreas o personas, por sus funciones y obligaciones, estarán autorizadas a acceder a las ubicaciones donde se encuentras los soportes.

Prueba 92.4:	Verificar que solo las personas autorizadas tienen acceso a los soportes que contienen datos de carácter personal.

Es necesario verificar qué medidas de seguridad existen en la Entidad para prevenir el acceso no autorizado:

- Acceso mediante llave física: revisar quién tiene el acceso a esta llave, donde se custodia y qué procedimiento existe de gestión de la llave.
- Acceso mediante tarjeta física: revisar quién tiene acceso y el mecanismo para la gestión de permisos de la tarjeta.
- Otros mecanismos, como los sistemas biométricos, será necesario revisar el procedimiento existente para la gestión de estos permisos.

Prueba 92.5:	Verificar que si existen limitaciones físicas, aparece reflejado en el Documento de Seguridad

Con algunos dispositivos puede que no sea posible la implementación exacta de algunos de los aspectos establecidos por el Reglamento de Desarrollo de la LOPD, por ello, es necesario identificar en el Documento de Seguridad si puede existir alguna limitación.

Prueba 92.6:	Determinar las salidas habituales de soportes que contengan datos de carácter personal.

Deberá existir un documento o anexo en el Documento de Seguridad donde se establezca la autorización de las salidas habituales de soportes que contengan datos de carácter personal.

Prueba 92.7:	Determinar las salidas eventuales de soportes que contengan datos de carácter personal.

Deberá existir un documento o anexo en el Documento de Seguridad donde se establezca la autorización de las salidas eventuales que se puedan producir de soportes que contengan datos de carácter personal.

Prueba 92.8:	Determinar las medidas de seguridad adoptadas en el traslado de soportes y/o documentación

Para ello, es necesario revisar los mecanismos utilizados para prevenir su sustracción, pérdida o acceso no autorizado:

- Valijas para el traslado de información de forma segura.
- Existencia de furgones o medios de transporte específicos.
- Utilización de mecanismos cerrados con llave / claves.
- Mecanismos utilizados para la protección de la información contenida en los soportes como cifrado de la información, medidas de control de acceso.

Prueba 92.9:	Determinar los modos de destrucción de documentos/soportes.

Algunos ejemplos de mecanismos para la destrucción de documentos/soportes son:

- Destructoras de papel y de soportes ópticos.
- Sistemas de desmagnetización de soportes que permitan el borrado no recuperable de los soportes.
- Mecanismos de destrucción física de los soportes.
- Contrato con empresas externas para llevar a cabo la destrucción segura de la información. Respecto a éstas es necesario tener en cuenta varios aspectos que se detallan en la siguiente prueba.

Prueba 92.10:	En caso de existir una externalización asociada a la destrucción de la información de forma segura, es necesario tener en cuenta ciertos aspectos mínimos de seguridad.

De esta forma verificar:

- Mecanismos empleados por la empresa externa.
- Existencia de contrato.
- Firma de cláusulas específicas en las que se incluya que la empresa externa no accederá en ningún caso a los soportes afectados.
- Existencia de certificado que asegure el borrado por parte de la empresa externa.

Prueba 92.11:	Verificar que para aquellos soportes que contengan información especialmente sensible se puedan utilizar mecanismos que impidan conocer a priori que información contienen.

En los casos de existir soportes que contengan información sensible de forma específica, será necesario verificar su etiquetado, ya que el Reglamento permite que para este tipo de soportes, se pueda implementar mecanismos que permitan identificar a los usuarios la información que contienen pero que para el resto de usuarios no sea fácil de identificar qué contienen dicha información.

6.4.1.5 Artículo 93. Identificación y autenticación

[1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento 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.
3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.
4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 93.1:	Verificar los mecanismos que permiten identificar/autenticar a los usuarios en los sistemas de información.

Para ello, identificar los métodos utilizados:

- Utilización de identificadores de usuarios corporativos y contraseñas de acceso a los sistemas de información.
- Mecanismos biométricos.
  Dentro de éstos se encuentran los sistemas de acceso a través de la huella dactilar, análisis de la retina, del iris, voz, vasculatura de la mano, etc..

  Es importante tener en cuenta que estos mecanismos no son completamente fiables, y que hay algunos como el sistema de identificación por análisis de la retina que se ha dejado de utilizar al poderse entender como una invasión a la intimidad dado que el escaneo puede revelar más información del afectado.

- Tarjetas físicas.

En cualquier caso, será necesario revisar cómo es el procedimiento de asignación de estos identificadores.

Prueba 93.2:	Verificar que para todos los sistemas de información que contengan datos de carácter personal no existan usuarios genéricos o compartidos.

Los usuarios genéricos o compartidos no permiten identificar qué usuario es el que está accediendo a la información, de esta forma, no permiten la identificación de forma inequívoca y personalizada de los usuarios.

Por ejemplo, existen determinadas aplicaciones y/o sistemas de información en los que existen distintos usuarios que pueden ser compartidos, es el caso, de un usuario de pruebas que se denomine “Pruebas” con el fin de identificar para qué es utilizado. En

estos casos, es necesario definir un procedimiento y/o control compensatorio para poder identificar la identidad de la persona que en cada momento está utilizando este usuario.

Prueba 93.3:	Verificar que exista un procedimiento de gestión de usuarios que incluya la solicitud, autorización, gestión y comunicación de las credenciales al usuario.

Este procedimiento debería incluir algún tipo de formulario en el que se incluyera el perfil del usuario, área o departamento y funciones asociadas de forma que se le dieran acceso únicamente a los sistemas de información necesarios para el desarrollo de sus funciones.

Este formulario debe ser cumplimentado por el responsable del área en el que vaya a desempeñar sus funciones.

Prueba 93.4:	Verificar que el mecanismo de distribución al usuario de su identificador y su contraseña sea seguro.

Una vez se haya generado el usuario, éste debe ser facilitado al usuario de forma segura, directamente al usuario.

Prueba 93.5:	Verificar que los sistemas de información disponen de mecanismos para garantizar la confidencialidad en el primer intento.

Los sistemas de información deben requerir cambiar la contraseña en su primer acceso, garantizando de esta forma que la contraseña ha sido cambiada por el usuario y que éste por tanto, es el único que la puede conocer.

De igual forma, los sistemas de información deben estar preparados para ocultar los caracteres en las pantallas de introducción de contraseñas, protegiendo las mismas de otros usuarios.

Prueba 93.6:	Verificar la periodicidad de cambio de la contraseña en todos los sistemas que contengan datos de carácter personal.

Es necesario tener en cuenta que:

- El valor puesto en los sistemas de información debe coincidir con el valor de periodicidad que se indique en el documento de seguridad.
- Y en todo caso es necesario tener en cuenta que será inferior a 12 meses

Prueba 93.7:	Verificar que las contraseñas se almacenan de forma cifrada en los sistemas de información.

Es necesario verificar que se encuentra cifrada y que no sea accesible.

6.4.1.6 Artículo 94. Copias de respaldo y recuperación

[1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.
2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.
Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.
3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.
4. 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 tratamiento realizado y se anote su realización en el documento de seguridad.
Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 94.1:	Verificar los procedimientos de realización de copias de respaldo y recuperación existentes

Para ello, será necesario identificar los distintos entornos y las herramientas que se utilizan para realizar las copias de respaldo.

Es necesario revisar cada herramienta para determinar:

- Procedimiento llevado a cabo para incluir un nuevo sistema de información en las políticas de realización de copias de respaldo.

  La necesidad de realización de la copia de respaldo tiene que partir del área de negocio responsable de dicho sistema de información, por lo que es necesario que exista un flujo de información de forma que desde negocio se indique a Tecnología las necesidades en cuanto a respaldo de la información.

- Tipo de copia de respaldo:
  - Full - completa
  - Incremental
  - Diferencial

- Definición de periodicidad, pudiendo establecerse:
  - Diaria
  - Semanal
  - Anual

Es importante destacar que el Reglamento establece que, mínimo se realizará una copia semanal salvo que en dicho período no hubiera habido ninguna modificación de los datos.

- Vigencia de las copias, tiempo de mantenimiento, rotación de las copias de respaldo.

- Determinar esquema de copias:

  - *Backup en un juego de una sola cinta*

    Es el esquema menos sofisticado, consiste en simplemente realizar la copia de seguridad en la misma cinta todos los días, sustituyendo ocasionalmente la cinta cuando se desgasta. Es muy sencillo de llevar a cabo, pero es necesario tener en cuenta que, si surge algún problema con el backup o la restauración, y si la cinta falla, no habría ninguna copia de seguridad.

    Desde el punto de vista de seguridad no se considera que sea un esquema adecuado.

  - *Esquema de rotación de cintas Round Robin*

    Este esquema consiste en tener cinco cintas de respaldo (una para cada día laborable de la semana) y utilizarlas de una en una sucesivamente. De ese modo, se utiliza la misma cinta cada día de la semana. Para mayor protección, se puede utilizar más de una cinta un día determinado de la semana, por ejemplo el viernes, y enviar una cinta del viernes fuera de la oficina cada semana, haciéndolas rotar.

    Este sistema requiere realizar un backup completo cada día.

  - *GFS ("grandfather"- "father"- "son")*

    El siguiente esquema de rotación de cintas más utilizado. Es sencillo y proporciona una buena protección con un número razonable de juegos de cintas.

    Existen numerosas variaciones del GFS que requieren distintos números de copias. Hacen falta de 8 a 22 juegos de cintas para realizar un backup de una semana laboral de cinco días si se conservan los datos de backup entre un mes y un año (o indefinidamente, si se hace rotar la cinta abuelo en la alineación en lugar de reciclarla).

    La versión más corriente de GFS consiste en realizar:
    - un backup diario (normalmente incremental) de lunes a jueves (el hijo)
    - un backup completo cada viernes (el padre).
    - a final de mes, se realiza otro backup completo y se conserva fuera de la sede (el abuelo).

- *Torre de Hanoi*

  La rotación en Torre de Hanoi es la más completa de las estrategias de rotación de cintas de uso corriente. Se caracteriza por añadir a la rotación un juego de cintas adicional que permite duplicar la duración del periodo de backup.

  Es útil cuando se necesita conservar backups que cubran un período de tiempo dilatado en un número de cintas razonable.

  El nombre del sistema procede de un puzzle del siglo XIX que demuestra los efectos de una explosión combinatoria. La rotación Torre de Hanoi aprovecha esa explosión combinatoria para ofrecer protección de datos. Con backups diarios, proporciona protección durante 2^(N-1) días, siendo N el número de juegos de cintas.

  El juego de cintas básico, al que llamaremos A, se utiliza para los backups de un día de cada dos. Con dos juegos de cintas, el segundo juego, al que llamaremos B, se utiliza en días alternos. Si añadimos un tercer juego, C, se alterna con B.

  Por lo tanto, una rotación de cuatro juegos sería como sigue:

  ABACABADABACABAD

  El sistema Torre de Hanoi hace un uso económico de las cintas, sobre todo si se desea conservar los backups durante un plazo de tiempo considerable. También refleja la realidad de que conforme se remonta hacia atrás en el tiempo disminuye la probabilidad de tener que recuperar a partir de la cinta, por eso los períodos de backup son progresivamente más largos.

- Seguridad de la herramienta, determinar quién puede acceder a dicha herramienta, cómo se gestionan los permisos sobre la misma.

- Custodia de las copias de respaldo:
  - Existencia de un robot físico.
  - Custodia externalizada.

- Informes de resultados obtenidos de la herramienta y cómo se gestionan las incidencias producidas en la realización de las copias de respaldo.

Prueba 94.2:	Verificar los procedimientos de recuperación de copias de respaldo y recuperación existentes.

Es necesario verificar los procedimientos establecidos de recuperación de copias de respaldo incluyendo:

- Canal de solicitud de recuperación de datos.
  Es necesario revisar el procedimiento de gestión de las recuperaciones de datos, qué usuarios pueden solicitar este tipo de peticiones y el canal habilitado para la recepción de las mismas.

- Existencia de personal autorizado para requerir una copia de respaldo.

- Canales de comunicación de la recuperación.
  El RLOPD establece que será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos en aquellos ficheros de nivel medio o alto.

Prueba 94.3:	Verificar la existencia de procedimientos de realización de copias de respaldo y recuperación para ficheros parcialmente automatizados (si los hubiere).

Verificar los procedimientos existentes de copias de respaldo, en concreto, si existe algún procedimiento referido a ficheros parcialmente automatizados.

Prueba 94.4:	Verificar la existencia de pruebas de verificación de las copias de respaldo.

Verificar la existencia de pruebas de verificación de las copias de respaldo:

- Pruebas de recuperación de entornos
- Peticiones asociadas a la recuperación de información de distintos entornos que permita verificar que la restauración ha sido realizada correctamente.
- Prueba semestral de recuperación de los distintos entornos existentes.

6.4.2 Sección II. Medidas de Seguridad de nivel medio

6.4.2.1 Artículo 95. Responsable de Seguridad

[En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.
En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 95.1:	Verificar la existencia de uno o varios Responsables de Seguridad.

Es necesario que en el Documento de Seguridad aparezca detallada la información acerca del Responsable de Seguridad, es necesario tener en cuenta que, tal y como se establece en el RLOPD esta figura podrá ser una persona o varias, teniendo que estar claramente descrito dichas figuras y su ámbito de responsabilidad en el Documento de Seguridad.

6.4.2.2 Artículo 96. Auditoría

[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 del presente título.
Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales 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 eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado 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, igualmente, 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 elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 96.1:	Verificar que se realiza una Auditoría de los sistemas de información que contienen datos de nivel medio o superior cada 2 años

La Auditoría bienal deberá verificar el cumplimiento de los aspectos y medidas de seguridad descritos en el RLOPD.

Prueba 96.2:	Verificar, si se identifica algún aspecto de carácter extraordinario, si se ha realizado la correspondiente auditoría con el fin de verificar las medidas de seguridad implantadas.

Es importante tener en cuenta que el Reglamento establece que será necesaria la realización de una Auditoría bienal o bien, una Auditoría si se ha producido algún hecho relevante que requiera la revisión del grado de cumplimiento de las medidas de seguridad.

Prueba 96.3:	Verificar si los informes de auditoría contienen la información mínima requerida por el RLOPD.

En concreto el Informe de Auditoría debe incluir:

- Detalle de las áreas revisadas.
- Hechos y observaciones.
- Identificación de deficiencias y medidas correctoras o aspectos necesarios a cumplir.

Prueba 96.4:	Verificar cómo se analizan los resultados de los informes de auditoría.

Es necesario que existan ciertas actividades con el fin de determinar que existe un adecuado control y seguimiento de las incidencias reportadas en el Documento de Seguridad:

- Son analizados por los distintos responsables de seguridad.
- Se han reportado las incidencias al Responsable del fichero con el fin de tomar medidas en la resolución de las incidencias detectadas.
- Existe un plan de acción/seguimiento de las recomendaciones indicadas en el informe con el fin de verificar que están implantando medidas de seguridad para subsanar las incidencias.

6.4.2.3 Artículo 97. Gestión de soportes y documentos

[1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 97.1:	Verificar que se dispone de un sistema de registro de las entradas de los soportes.

Es necesario que exista un registro en el que se incluya el detalle de las entradas de soportes que existen en la Entidad.

Prueba 97.2:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Tipo de documento o soporte: El soporte o documento podrá ser en Papel, fichero electrónico, CD, DVD, pen-drive, etc.

Prueba 97.3:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Fecha y hora.

Prueba 97.4:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Emisor: persona autorizada encargada de enviar el soporte.

Prueba 97.5:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Número de documentos o soportes.

Prueba 97.6:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Tipo de información que contienen los soportes.

Prueba 97.7:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Forma de envío.

Prueba 97.8:	Verificar que se dispone de un sistema de registro de las entradas de soportes que contenga la información requerida.

En concreto debe contener:

- Responsable de recepción - persona que se encargará de su recepción.

Prueba 97.9:	Verificar que el Documento de Seguridad contiene una autorización para las personas responsables de la recepción del soporte.

Verificar que el Documento de Seguridad contiene la relación de personas autorizadas a la recepción del soporte.

Prueba 97.10:	Verificar que se dispone de un sistema de registro de las salidas de los soportes.

Verificar que se dispone de un registro de la salida de los soportes. Este registro deberá disponer de determinada información que se detallará en las siguientes pruebas.

Prueba 97.11:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Tipo de documento o soporte: Papel, fichero electrónico, CD, DVD.

Prueba 97.12:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Fecha y hora.

Prueba 97.13:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Destinatario: a quien va dirigido el soporte.

Prueba 97.14:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Número de documentos o soportes.

Prueba 97.15:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Tipo de información que contienen los soportes.

Prueba 97.16:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Forma de envío

Prueba 97.17:	Verificar que se dispone de un sistema de registro de las salidas de soportes, que contenga la información requerida.

En concreto debe contener:
- Responsable de la entrega

Prueba 97.18:	Verificar que el Documento de Seguridad contiene una autorización para las personas responsables de la salida del soporte.

Deberá contener una autorización, anexo o referencia a la misma.

6.4.2.4 Artículo 98. Identificación y autenticación

[El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 98.1:	Verificar que los sistemas de información disponen de mecanismos que permitan limitar el número de intentos no permitidos a los sistemas de información.

Como buenas prácticas se recomienda que este valor se encuentre entre 3-5.

6.4.2.5 Artículo 99. Control de acceso físico

[Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 99.1:	Verificar que el Documento de Seguridad contiene una relación del personal autorizado a acceder a los lugares donde se hallen instalados los equipos que den soporte a los sistemas de información.

Es necesario tener en cuenta que hay que revisar la adecuación de los sistemas de control de acceso físico que permitan restringir el acceso únicamente a la relación de personas autorizadas que aparezcan en el Documento de Seguridad.

Además es necesario que se distingan todas las áreas en las que pueden existir sistemas de información:

- Centros de Procesamiento de Datos.
- Salas donde se ubiquen las copias de respaldo.

Si bien, la LOPD no incluye otros aspectos relativos al acondicionamiento de estas salas, sí se considera adecuado realizar una revisión de las medidas de seguridad

medioambiental que pueden disponer los recintos donde haya sistemas de información que contengan datos de carácter personal.

Es necesario valorar la existencia de:

- Cámaras de videovigilancia.
- Medidas de Seguridad anti-incendios.
- Detectores de humedad.
- Detectores de terremotos.
- Medidas de control de la temperatura y aire acondicionado para mantener los servidores a una temperatura adecuada.
- Existencia de SAIs (Servicio de Alimentación Interrumpida).

6.4.2.6 Artículo 100. Registro de incidencias

[1. En el registro regulado en el artículo 90 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.
2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 100.1:	Verificar que el registro de incidencias incluye las incidencias de recuperación de datos.

El registro de incidencias de la Entidad deberá tener identificadas las incidencias de recuperación de datos.

Prueba 100.2:	Verificar que en el registro de incidencias se incluye la información exigida por el RLOPD

En concreto la información que se debe incluir es:
- los procedimientos realizados de recuperación.

Prueba 100.3:	Verificar que en el registro de incidencias se incluye la información exigida por el RLOPD

En concreto la información que se debe incluir es:
- Persona que ejecutó el proceso.

Prueba 100.4:	Verificar que en el registro de incidencias se incluye la información exigida por el RLOPD

En concreto la información que se debe incluir es:
- Datos restaurados.

Prueba 100.5:	Verificar que en el registro de incidencias se incluye la información exigida por el RLOPD

En concreto la información que se debe incluir son:
- qué datos ha sido necesario grabar manualmente (en su caso).

Prueba 100.6:	Verificar que las recuperaciones de datos que contengan datos de nivel medio han sido autorizadas por el responsable del fichero.

Para ello, es necesario verificar el flujo de aprobación de dichas recuperaciones, en el Documento de Seguridad tendrá que aparecer en quiénes tiene delegado el Responsable del Fichero esta autorización y habrá que verificar que en efecto, dichas personas son las encargadas de realizar esta autorización previa la recuperación de la información.

6.4.3 Sección III. Medidas de Seguridad de nivel Alto

6.4.3.1 Artículo 101. Gestión y distribución de soportes

[1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.
2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.
Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.
3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 101.1:	Verificar que los soportes dispongan de sistemas de etiquetado comprensibles para los usuarios autorizados a acceder a los mismos y que dificulten el acceso para el resto de usuarios.

Verificar el sistema de etiquetado empleado por la entidad, el mismo debe ser comprensible para la entidad (por ejemplo a través de un código de barras o etiqueta con la referencia) pero no debe facilitar el acceso al resto de usuarios.

Prueba 101.2:	Verificar que si existe una distribución de soportes que contengan datos de carácter personal, esta distribución se realiza cifrando los datos o bien usando otro mecanismo que garantice que la información no sea accesible ni manipulada durante su transporte.

Será necesario valorar si, la distribución no se realiza de forma cifrada, los mecanismos empleados para verificar la inaccesibilidad que indica el RLOPD, de esta forma será necesario valorar:

- Medidas físicas: armario cerrado, personal restringido, maletines cerrados, etc.
- Medidas lógicas: canal seguro de transmisión.

Prueba 101.3:	Verificar que en el caso de utilizarse dispositivos portátiles que contengan datos de nivel alto, se utiliza alguna herramienta de cifrado de la información.

Verificar los mecanismos utilizados de cifrado de dispositivos portátiles.

Prueba 101.4:	Verificar los mecanismos utilizados de encriptación de dispositivos portatiles, si no se dispone de mecanismos deberá estar detallado en el Documento de Seguridad y será necesario incluir medidas apra minimar los riesgos.

Verificar que, si no se dispone de mecanismos, deberá estar detallado en el Documento de Seguridad y será necesario incluir medidas compensatorias para minimizar los riesgos.

6.4.3.2 Artículo 102. Copias de respaldo y recuperación

[Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 102.1:	Verificar que existe una ubicación alternativa para la información relativa a los sistemas de información de nivel alto.

La copia deberá almacenarse en otro lugar, puede tratarse de un CPD alternativo que se dispongo, u otro centro que disponga la Entidad.

Prueba 102.2:	Verificar que la ubicación alternativa para almacenar los datos de nivel alto cumple los aspectos requeridos.

La ubicación alternativa debe disponer de medidas de control de acceso físico además de contar con medidas de seguridad medioambiental.

6.4.3.3 Artículo 103. Registro de accesos

[1. De cada intento de 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.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a. Que el responsable del fichero o del tratamiento sea una persona física.
b. Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 103.1:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene identificación del usuario que accede.

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Identificación del usuario que accede.

Prueba 103.2:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene la fecha y la hora del acceso.

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Identificación de la fecha y la hora en la que se ha producido el acceso al registro que contiene los datos de nivel alto.

Prueba 103.3:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene el fichero accedido.

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Identificación del fichero accedido que contiene los datos de nivel alto.

Prueba 103.4:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene el tipo de acceso (lectura/escritura)

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Indicación del tipo de acceso que se haya producido a los datos de nivel alto, distinguir entre lectura y escritura.

Prueba 103.5:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene si el acceso fue autorizado o denegado.

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Indicación si el acceso fue autorizado o denegado.

Prueba 103.6:	Verificar que en cada aplicación/sistema de información que contenga datos de carácter personal de nivel alto existe un registro de accesos que contiene si el acceso fue autorizado una identificación del registro en concreto al que se ha accedido.

Verificar que el registro de acceso contiene la información requerida, en concreto contiene:

- Indicación del registro accedido.

Prueba 103.7:	Verificar que no es parametrizable el registro de accesos de forma que siempre esté activo y solo pueda ser manipulado por el responsable de Seguridad.

Verificar que el registro de acceso se encuentra en un lugar de acceso restringido al responsable de seguridad para poder llevar a cabo la revisión del registro de acceso y que éste no se puede desactivar ni modificar.

Prueba 103.8:	Verificar que el registro de accesos se conserva durante un período de 2 años.

Verificar que el registro de acceso se tiene que conservar un período de 2 años, por lo que se tendrá que mantener en un a ubicación con acceso restringido en ese período de tiempo.

Prueba 103.9:	Verificar que mínimo una vez al mes, el responsable de seguridad se encarga de revisar los registros de accesos y emite un informe con las incidencias y/o problemas detectados.

Verificar que el responsable de seguridad realiza una vez al mes la revisión del registro de accesos, emitiendo un informe con las incidencias detectadas.

Prueba 103.10:	Verificar si la entidad no obtiene el registro de acceso porque se cumplan los dos aspectos indicados

La excepción que ofrece el Reglamento relativo a la obtención del registro de acceso, obliga a que se den estas dos circunstancias:

- Responsable del Fichero sea una persona física, por ejemplo un autónomo.
- Responsable del Fichero puede garantizar que únicamente él mismo accede y trata los datos de carácter personal.

En estos casos, tal y como se establece en el RLOPD, no sería necesario un Registro de Accesos, dado que la entidad sería unipersonal y solo la misma persona accedería a la información de carácter personal.

6.4.3.4 Artículo 104. Telecomunicaciones

[Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 104.1:	Verificar que si se realiza transmisión de datos a través de redes públicas o inalámbricas existen procedimientos de cifrado de la información u otro mecanismo para garantizar que la información no sea inteligible ni manipulada por terceros.

Verificar las transmisiones de datos que se produzcan desde la entidad:

- Existencia de información vía protocolo FTP ó FTPs.
- Métodos de intercambio de información vía EDITRAN.
- Intercambio de información por correo electrónico.
- Intercambio de información a través de páginas web.

Cualquiera de los métodos utilizados deberá verificarse que se utilizan protocolos de intercambio de información seguros y/o que la información se envía cifrada.

6.5 Capítulo IV. Medidas de Seguridad aplicables a los ficheros y tratamientos no automatizados

6.5.1 Sección I. Medidas de Seguridad de nivel Básico

6.5.1.1 Artículo 105. Obligaciones comunes

[1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:
a. Alcance.
b. Niveles de seguridad.
c. Encargado del tratamiento.
d. Prestaciones de servicios sin acceso a datos personales.
e. Delegación de autorizaciones.
f. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g. Copias de trabajo de documentos.
h. Documento de seguridad.
2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a. Funciones y obligaciones del personal.
b. Registro de incidencias.
c. Control de acceso.
d. Gestión de soportes.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 105.1:	Es necesario revisar el cumplimiento de los aspectos de obligación comunes a los ficheros automatizados.

En concreto las medidas relacionadas con:

- Alcance y niveles de seguridad.
- Encargado del tratamiento.
- Prestaciones de servicios sin acceso a datos personales.
- Delegación de autorizaciones.
- Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
- Copias de trabajo de documentos.
- Documento de Seguridad.

De esta forma, la revisión de éstas medidas de seguridad, que se regulan en los correspondientes artículos, serán de cumplimiento tanto en ficheros automatizados como en ficheros no automatizados.

Prueba 105.2:	Es necesario revisar el cumplimiento de los aspectos de obligación comunes a los ficheros automatizados

En concreto, se deberán revisar las medidas relacionadas con:

- Funciones y obligaciones del personal.
- Registro de incidencias.
- Control de acceso.
- Gestión de soportes.

Al igual que en la prueba anterior, la revisión de las medidas de seguridad de dichos apartados también serán comunes a ficheros automatizados y ficheros no automatizados

6.5.1.2 Artículo 106. Criterios de archivo

[El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación
En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 106.1:	Verificar que se hayan definido los correspondientes criterios de archivo para cada uno de los ficheros no automatizados o mixtos existentes.

Existencia de plantilla o similar en que se identifique cada uno de los archivos y se incluya:

- Localización.
- Personal con acceso.
- Documentación existente.
- Criterios de ordenación.

Prueba 106.2:	Verificar que los criterios adoptados permiten garantizar la conservación de los documentos

En concreto, es necesario comprobar:

- Armarios, salas sean adecuados en cuanto a condiciones medioambientales y medidas de control de acceso.

Prueba 106.3:	Verificar que los criterios adoptados permiten garantizar la localización y consulta de la información.

En concreto, es necesario comprobar:

- La información está accesible, etiquetada y que fácilmente se puede localizar y/o consultar la información requerida.

Prueba 106.4:	Verificar que los criterios adoptados permiten el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

Para realizar esta prueba es necesario tener en cuenta que:

- la información debe ser accesible y localizable, de esta forma, a partir de determinada información, será necesario poder localizar donde se encuentra archivado físicamente para poder ejercitar el derecho correspondiente.
- Posible custodia de la información en archivos externos, siendo necesario de igual forma su localización.

6.5.1.3 Artículo 107. Dispositivos de almacenamiento

[Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 107.1:	Verificar donde se almacenan los documentos

Verificar la existencia de documentación en armarios, cajoneras, archivos departamentales o centrales, y adicionalmente revisar las medidas existentes para prevenir el acceso no autorizado:

- Entrada por tarjeta
- Con llave física.
- Existencia de otros dispositivos.

6.5.1.4 Artículo 108. Custodia de los soportes

[Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 108.1:	Verificar las áreas donde se tratan ficheros con datos de carácter personal en papel.

Revisar donde se custodia esta información cuando se encuentra en proceso de revisión o trámite. Identificar cajoneras o armarios departamentales que impidan el acceso a la información por parte de personal no autorizado.

Es necesario también adoptar medidas para que el personal no deje la documentación encima de las mesas sin ningún tipo de control de acceso.

6.5.2 Sección II. Medidas de Seguridad de nivel Medio

6.5.2.1 Artículo 109. Responsable de Seguridad

[Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 109.1:	Verificar que se identifiquen en el Documento de Seguridad el/los responsables de Seguridad existentes en lo referente a las medidas de seguridad a aplicar a ficheros no automatizados.

De igual forma a como se establece en el artículo 95, deberá existir esta figura con independencia de si el fichero está automatizado o no automatizado.

6.5.2.2 Artículo 110. Auditoría

[Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 110.1:	Verificar que los ficheros no automatizados están sometidos a una Auditoría bienal que verifique el cumplimiento de las medidas de seguridad correspondientes.

De igual forma a como se establece en el artículo 96, se deberá llevar a cabo una Auditoría bienal que contemple el grado de cumplimiento de la entidad con independencia de si los fichero están en soporte automatizado o no automatizados.

6.5.3 Sección III. Medidas de Seguridad de nivel Alto

6.5.3.1 Artículo 111. Almacenamiento de la información

[1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.
2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 111.1:	Verificar que los armarios, archivadores u otros se encuentran en áreas de acceso restringido a través de llave u otro dispositivo equivalente

Verificar las medidas de control de acceso que áreas dispongan: existencia de tarjetas, llaves, biométricos, que aseguren que el acceso a la información esté restringida.

Prueba 111.2:	Verificar que dichas áreas permanecen cerradas cuando no sea preciso acceder a las áreas donde se encuentran los documentos.

Verificar que las áreas se encuentran cerradas:

- en diferentes períodos de la jornada laboral
- los sistemas mediante tarjeta no se habilita el acceso por defecto a las salas donde exista la información.

Prueba 111.3:	Verificar si el RF indica que no es posible cumplir con las medidas requeridas en cuanto al almacenamiento de la información, las medidas alternativas que se han adoptado

Verificar que, si existen excepciones de cumplimiento en cuanto al almacenamiento de la información, se haya incluido medidas alternativas:

- que conste la existencia de medidas alternativas
- valorar la adecuación de dichas medidas

Prueba 111.4:	Verificar que las medidas alternativas se encuentran descritas en el Documento de Seguridad.

Verificar que, si existen excepciones de cumplimiento en cuanto al almacenamiento de la información, se hayan incluido y se encuentren correctamente documentadas en el Documento de Seguridad.

6.5.3.2 Artículo 112. Copia o reproducción

[1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.
2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 112.1:	Verificar que existe personal autorizado para generar copias o reproducir documentos que contengan datos de carácter personal de nivel alto.

Verificar que existe una relación de personas autorizadas a realizar copias o reproducciones de la información y que constan procedimientos para garantizar que este listado se encuentra debidamente actualizado.

Prueba 112.2:	Verificar que el personal autorizado para generar copias o reproducir documentos que contengan datos de carácter personal de nivel alto se ha incluido en el Documento de Seguridad.

Verificar que la relación de personas autorizadas a realizar copias o reproducciones de la información se haya incluido en el Documento de Seguridad.

Prueba 112.3:	Verificar los mecanismos empleados para la destrucción segura de documentación de nivel alto

En concreto, verificar la utilización de:

- Destructoras de papel.
  Es importante tener en cuenta normativas específicas para asegurar la destrucción segura del papel: DIN 66399, y norma española UNE 15713:2010

- Contratos con Proveedores especializados.

6.5.3.3 Artículo 113. Acceso a la documentación

[1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 113.1:	Verificar que el acceso a la documentación se limite al personal autorizado.

Verificar que existe una relación de personas autorizadas a acceder a la documentación y que constan procedimientos para garantizar que este listado se encuentra debidamente actualizado.

Prueba 113.2:	Verificar que se hayan establecido mecanismos para identificar los accesos realizados por distintas personas a la documentación, por ejemplo mantenimiento de un registro de quien ha accedido a la documentación en un momento concreto.

Verificar que existe un registro de acceso para identificar las personas con acceso a la información en un momento concreto:

- identificar quién ha accedido a la sala y a qué documentación

- identificar la fecha y hora de dicho acceso.

Prueba 113.3:	Verificar los mecanismos existentes para detectar y controlar el acceso no autorizado a la documentación.

Verificar que existe un registro de acceso para identificar los posibles accesos no autorizados:

- identificar intentos de acceso a la salas donde se ubique la información
- revisión periódica de que usuarios han accedido a la sala y a qué documentación, y si disponían de autorización para ello.

6.5.3.4 Artículo 114. Traslado de documentación

[Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.]

Pruebas de Auditoría:

Las pruebas de auditoría que considero necesarias para verificar su cumplimiento son las siguientes:

Prueba 114.1:	Verificar las medidas a implantar en el traslado físico de la documentación que contenga datos de nivel alto para impedir el acceso o manipulación de la información.

De entre las medidas a implantar se pueden encontrar:

- Sellado de Documentación.
- Cierre de sacas que contengan Documentación.
- Revisión por parte del personal correspondiente para verificar que no ha habido manipulación durante el traslado.

Capítulo 7

Evolución normativa de protección de datos

7.1 Reformas legislativas

Desde la entrada en vigor el 19 de marzo de 2008 del 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 (en adelante, RLOPD), la actividad legislativa ha sido prolífera, y muchas de estas nuevas normas han afectado, en uno u otro sentido, a la normativa sobre protección de datos.

Las normas que con su entrada en vigor han afectado a la normativa sobre protección de datos son las siguientes:

- La Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema de Seguridad Nacional.
- Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio.

A continuación se analizan los cambios producidos en materia de protección de datos por estas nuevas normativas, así como las disposiciones afectadas.

7.1.1 La Ley 2/2011, de 4 de marzo, de Economía Sostenible

La Disposición final quincuagésima modificada determinados artículos de la Ley Orgánica de 13 de diciembre, sobre Protección de Datos de Carácter Personal (en adelante, LOPD).

En concreto se modifican los siguientes artículos:

Artículo	Acción realizada
43 de la LOPD	Modificación del apartado 2
44 de la LOPD	Modificación de los apartados. 2, 3 y 4.
45 de la LOPD	Modificación de los apartados del 1 al 5. Inclusión del apartado 6. Modificación de los apartados 6 y 7, que pasan a ser 7 y 8.
46 de la LOPD	Modificación de los apartados 1, 2 y 3.

Tabla 3: Modificaciones producidas por la Ley 2/2011

Todas estas modificaciones tienen por objeto aportar una mayor seguridad jurídica y mayor precisión en la aplicación de la norma, así como ampliar los criterios de modulación y adecuación de sanciones.

A continuación, se describen cada una de las modificaciones, para ello se han marcado en el texto en color rojo en el propio texto del artículo.

Tras indicar el cambio realizado, se realizará una explicación de lo que conlleva dicha modificación.

Artículo 43 de la LOPD

Este artículo describe información relativa a los Responsables:

[Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

1. *Cuando se trate de ficheros de titularidad pública se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en los artículos 46 y 48 de la presente Ley.]*

Artículo 44 de la LOPD

En dicho artículo se establece qué conductas son constitutivas de infracción y su grado: leve, grave o muy grave.

[1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

- *a) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo*
- *b) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos.*

c) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean recabados del propio interesado.
d) La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el artículo 12 de esta Ley.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.
b) Tratar datos de carácter personal sin recabar el consentimiento de las personas afectadas, cuando el mismo sea necesario conforme a lo dispuesto en esta ley y sus disposiciones de desarrollo.
c) Tratar datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en el artículo 4 de la presente Ley y las disposiciones que lo desarrollan, salvo cuando sea constitutivo de infracción muy grave.
d) La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley.
e) El impedimento o la obstaculización del ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
f) El incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos no hayan sido recabados del propio interesado.
g) El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo.
h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
i) No atender los requerimientos o apercibimientos de la Agencia Española de Protección de Datos o no proporcionar a aquélla cuantos documentos e informaciones sean solicitados por la misma.
j) La obstrucción al ejercicio de la función inspectora.
k) La comunicación o cesión de los datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo, salvo que la misma sea constitutiva de infracción muy grave.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa o fraudulenta.
b) Tratar o ceder los datos de carácter personal a los que se refieren los apartados 2, 3 y 5 del artículo 7 de esta Ley salvo en los supuestos en que la misma lo autoriza o violentar la prohibición contenida en el apartado 4 del artículo 7.
c) No cesar en el tratamiento ilícito de datos de carácter personal cuando existiese un previo requerimiento del Director de la Agencia Española de Protección de Datos para ello.
d) La transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria»]

A continuación, explicaremos las modificaciones llevadas a cabo:

- <u>Modificaciones relacionadas con las infracciones leves</u>:

  - Desaparecen dos infracciones:
    - No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.
    - Incumplir el deber de secreto (salvo que constituya infracción grave).

  - Se añade una nueva infracción: “La transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales establecidos en el

artículo 12 de esta Ley", que supone penalizar la conducta consistente en facilitar datos de carácter personal a un encargado del tratamiento por parte del responsable del fichero sin que medie el contrato y forma que exige el artículo 12 de la LOPD. Ahora se castiga expresamente no firmar dicho contrato.

- Modificaciones relacionadas con las infracciones graves:

  - Se atenúa la cesión de datos, pasando a ser castigadas como infracción grave. La calificación de "muy grave" se utilizará para casos muy concretos.

  - Se añade una nueva infracción grave: "El incumplimiento de los restantes deberes de notificación o requerimiento al afectado impuestos por esta Ley y sus disposiciones de desarrollo" donde podrán encajar diversas conductas desobedientes.

  - Se agrava la infracción del deber de secreto, pasando de ser leve a grave.

- Modificaciones relacionadas con las infracciones muy graves

  - Se simplifican y reducen significativamente este tipo de infracciones, pasando de ser 9 conductas castigadas como infracción muy grave, a ser 4 en la actualidad.

  - Desaparece la cesión de datos en general, constituyendo infracción muy grave únicamente cuando los datos objeto de cesión se refieran a los indicados en los apartados 2, 3 y 5 del artículo 7.

  - Desaparece la posibilidad de vulnerar en el deber de secreto de forma muy grave cuando los datos hacían referencia a los mismos supuestos que el caso anterior.

  - Desaparece la infracción consistente en no atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero y obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición (conductas que podrán ser constitutivas de infracción grave pues encajarían en el nuevo tipo infractor de esta categoría).

Artículo 45 de la LOPD

En dicho artículo se establecen los tipos de sanciones y las cuantías de las mismas.

[Las infracciones leves serán sancionadas con multa de 900 a 40.000 euros.
1. Las infracciones graves serán sancionadas con multa de 40.001 a 300.000 euros.
2. Las infracciones muy graves serán sancionadas con multa de 300.001 a 600.000 euros.
3. La cuantía de las sanciones se graduará atendiendo a los siguientes criterios:
   a) El carácter continuado de la infracción.
   b) El volumen de los tratamientos efectuados,
   c) La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.
   d) El volumen de negocio o actividad del infractor.
   e) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
   f) El grado de intencionalidad.
   g) La reincidencia por comisión de infracciones de la misma naturaleza.

h) La naturaleza de los perjuicios causados a las personas interesadas o a terceras personas,

i) La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

j) Cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

4. El órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia, de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

d) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

e) Cuando se hay producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

5. Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.]

Las modificaciones son las siguientes:

- <u>Modificaciones relacionadas con la cuantía de las sanciones:</u>

  - Sanciones leves: se modifica el tramo de la cuantía, incrementando el importe mínimo (pasando de ser de 601,01 a 900 euros), y reduciendo el importe máximo (pasando de ser de 60.101,21 a 40.000 euros).

  - Sanciones graves: al modificar el tramo superior de las sanciones leves, se modifica el importe del mínimo de este tramo, pasando de ser de 60.101,21 a 40.000 euros.

  - Sanciones muy graves: aquí las modificaciones se producen a la hora de redondear las cuantías de este tramo, ya que los importes anteriores (300.506,05 euros a 601.012,10 euros) se calcularon convirtiendo las cifras en pesetas, y poniendo su equivalencia en euros. Tras esta actualización el importe de las sanciones queda, por tanto, comprendido en el tramo de 300.001 a 600.000 euros.

- Modificaciones relacionadas con criterios para graduar las sanciones

  Se han reformado y añadidos nuevos criterios para graduar las sanciones. Así, ahora se tendrá en cuenta:

  - El carácter continuado de la infracción.

  - La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

  - El volumen de negocio o actividad del infractor.

  - La acreditación de que con anterioridad a los hechos constitutivos de infracción la entidad imputada tenía implantados procedimientos adecuados de actuación en la recogida y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

- Modificaciones relacionadas con criterios para atenuar las sanciones

  Se elimina la antigua mención del artículo 45.5 de la LOPD y se añaden una serie de atenuantes, que procederán:

  - Cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el apartado 4 de este artículo.

  - Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

  - Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

  - Cuando el infractor haya reconocido espontáneamente su culpabilidad.

  - Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente.

- Introducción de la figura del apercibimiento

  Entre estas modificaciones la más destacada podría ser la figura del apercibimiento, como medida preventiva no sancionadora, que se regula en el artículo 45.6 de la LOPD.

  Esta medida, de carácter excepcional y limitada, deberá fundarse en la especial concurrencia de los criterios previstos para la atenuación de sanciones, podrá permitir advertir de a irregularidad cometida y requerir la adopción de las adecuadas medidas que peritan, en cada caso, corregir la situación o evitar la repetición de dicha conducta.

  Con esta medida el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo

que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en la LOPD.
b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 46 de la LOPD

Relativo a las infracciones se las administraciones públicas.

[1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador 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 órgano sancionador 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 al órgano sancionador 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.]

Artículo 49 de la LOPD

Este artículo describe información relativa a la potestad de inmovilizar ficheros:

[En los supuestos, constitutivos de infracción grave o muy grave en que la persistencia en el tratamiento de los datos de carácter personal o su comunicación o transferencia internacional posterior pudiera suponer un grave menoscabo de los derechos fundamentales de los afectados y en particular de su derecho a la protección de datos de carácter personal, el órgano sancionador podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.
Si el requerimiento fuera desatendido, el órgano sancionador podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.]

Se amplía esta facultad de la AEPD a los casos de infracciones graves, cuando antes sólo se aplicaba a las infracciones muy graves.

7.1.2 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

La Disposición adicional cuarta modifica la letra b) del apartado 5 del artículo 81 del RLOPD, elimina el concepto de “no automatizados”:

[5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:
a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.]

Con la eliminación del concepto "no automatizados" se amplía la excepción de implantar medidas de seguridad de nivel alto en determinados ficheros con datos sensibles contenida en dicho artículo.

Por lo que dicha excepción (específica para los ficheros o tratamientos no automatizados), se convierte después de la modificación introducida en una excepción general aplicable a todo tipo de ficheros, independientemente de cual sea su forma de soporte.

7.1.3 Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la Ley sobre el libre acceso a las actividades de servicios y su ejercicio

La Disposición adicional sexta de esta Ley, más conocida como Ómnibus, permite a cualquier empresa o particular realizar las actividades de vender, entregar, instalar y mantener equipos técnicos de seguridad, sin necesidad de cumplir los requisitos previstas en la Ley de Seguridad Privada para tales empresas, como puede ser la autorización del Ministerio del Interior.

No obstante, la instalación de un sistema de videovigilancia conectado a una central de alarma, sí seguirá requiriendo la concurrencia de los requisitos exigidos hasta ahora; esto es, que el dispositivo sea contratado, instalado y mantenido por una empresa de seguridad privada autorizada por el Ministerio del Interior y que el contrato sea notificado a dicho Departamento.

Sin embrago, la Agencia Española de Protección de Datos recoge en su Informe Jurídico 0650/2009, que el tratamiento de las imágenes realizado mediante los sistemas de videovigilancia, independientemente de cual sea la naturaleza de la empresa, deberá cumplir con los requisitos exigibles en materia de protección de datos de carácter personal, recogidos en tanto en la LOPD como en la demás normativa de desarrollo.

De forma particular, en la Instrucción 1/2006 de la Agencia Española de Protección de Datos, en relación al tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras se establece que se deberá cumplir con lo relativo a:

- Que las imágenes que se capten sean las necesarias y no excesivas para la finalidad perseguida.
- El deber de informar a los interesados, tanto a través de la colocación de carteles informativos.
- Puesta a disposición de impresos en los que se detalle la información.
- La notificación de la existencia de los ficheros a la AEPD.

- La implantación de medidas de seguridad.

7.2 Sentencia del Tribunal Supremo de la Sala 3ª

En determinadas ocasiones el legislador no va a ser el que modifique el texto de la norma vigente, sino que van a ser los Tribunales de Justicia, a través de las resoluciones dictadas por sus miembros, los que se van a encargar de realizar esta función por ser disconformes a derecho.

Entre este tipo de resoluciones se encuentra la Sentencia de la Sala 3ª del Tribunal Supremo de fecha 15 de julio de 2010, que modifica los siguientes artículos:

Artículo	Acción realizada
11 del RLOPD	Anulación íntegra del artículo
18 del RLOPD	Anulación íntegra del artículo
38 del RLOPD	Se anula parte del epígrafe 1.a) Se anula el epígrafe 2 entero
123 del RLOPD	Se anula el epígrafe 2 entero

Artículo 11 del RLOPD

El artículo 11 del RLOPD, establecía, en relación a la verificación de datos en solicitudes formuladas a las Administraciones públicas:

[Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos.]

Este artículo, ha sido anulado al considerar el Tribunal que este artículo permitía la verificación por las Administraciones Públicas de datos en solicitudes formuladas por los ciudadanos sin requerir consentimiento de estos, habilitando una cesión de datos al margen de los supuestos autorizados por los artículos 6 y 11 de la LOPD.

La declaración de nulidad del precepto conlleva una garantía de protección de los datos de personas físicas ante la gestión de las Administraciones Públicas, pero también una incomodidad para el ciudadano, que deberá volver a declarar los datos personales de que se trate o acreditar su autenticidad.

Artículo 18 del RLOPD

El artículo 18 del RLOPD en relación a la acreditación del cumplimiento del deber de información establecía lo siguiente:

[1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.
2. El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.]

Este artículo ha sido anulado porque, en este caso, el Tribunal ha entendido que la LOPD establece la libertad de forma tanto para la prueba de la obtención del consentimiento del interesado, como para la acreditación del cumplimiento del deber de información al mismo, por lo que no se pueden establecer obligaciones adicionales al margen de lo que establece la normativa sobre protección de datos.

La sentencia da el razonamiento de la siguiente manera:

[La Ley reconoce en el artículo 5 el derecho a la información en la recogida de datos, concreta el contenido de la información, y advierte de que el deber de informar ha de ser previo a la recogida, pero salvo la indicación de que la información ha de ser expresa, precisa e inequívoca, ninguna referencia contiene a la forma, abriendo así múltiples posibilidades (escrita, verbal, telemática, etc.) Sólo en el apartado 2 del artículo de mención prevé la posibilidad de que se utilicen cuestionarios u otros impresos para la recogida de datos para advertir, pensando sin duda en medios estandarizados, que se han de contener y de forma claramente legible las advertencias expresadas en el apartado 1.

En consecuencia, debe considerarse que el legislador ha optado por la libertad de forma.
Pues bien, siendo ello así, cabe concluir que la disposición reglamentaria que examinamos contraviene la Ley y que por ello debe ser anulada.]

Artículo 38 del RLOPD

En este artículo se establecen los requisitos para la inclusión de los datos en ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, se modifica lo siguiente:

["Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:
a. Existencia previa de una deuda cierta, vencida, exigible, que haya resultado ~~impagada y respecto de la cual no se haya entablado reclamación judicial, arbitral "o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero~~"
b. Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.
c. Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.
~~1. No podrán incluirse en los ficheros de esta naturaleza datos personales sobre los que exista un principio de prueba que de forma indiciaria contradiga alguno de los requisitos anteriores.~~
~~Tal circunstancia determinará asimismo la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado su inclusión en el fichero.~~
2. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación

suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.]

Se modifican los siguientes aspectos:

- Respecto al epígrafe 1º la anulación de la frase viene producida por la inseguridad jurídica que generaba su redacción, al considerar que no se concretaba qué procedimientos justificaban la no inclusión de las deudas en los ficheros de solvencia económica, y al permitir considerar que la reclamación formulada por el propio acreedor impedía la inclusión de los datos en el fichero al no poder considerarse la deuda como "cierta" (indubitada).

- En relación a la anulación del epígrafe 2º, se debe a que se crea una inseguridad jurídica al trasladar la carga de la prueba de la concurrencia de los requisitos previstos en el epígrafe anterior al encargado del tratamiento, y al no concretar qué principio de prueba exige (documental, pericial, testifical, etc.), junto a la dificultad de apreciación del grado exigible de la prueba indiciaria.

Artículo 123 del RLOPD

El artículo 123 del RLOPD en relación al personal competente para la realización de actuaciones previas, se modifica lo siguiente:

[Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

1. *~~En supuestos excepcionales, el Director de la Agencia Española de Protección de Datos podrá designar para la realización de actuaciones específicas a funcionarios de la propia Agencia no habilitados con carácter general para el ejercicio de funciones inspectoras o a funcionarios que no presten sus funciones en la Agencia, siempre que reúnan las condiciones de idoneidad y especialización necesarias para la realización de tales actuaciones. En estos casos, la autorización indicará expresamente la identificación del funcionario y las concretas actuaciones previas de inspección a realizar.~~*
2. *Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.*
   Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.]

Las modificaciones son las siguientes:

- Se anula el epígrafe 2 al considerar el Tribunal que se faculta al Director de la AEPD con una libertad, como es la de poder designar el personal para el ejercicio de la función inspectora, que no se prevé de la encomienda de gestión que se establecen en los artículos 35, 37 y 40 de la LOPD.

7.3 Posturas doctrinales de la Agencia Española de Protección de Datos

Una de las funciones que tiene la Agencia Española de Protección de Datos es responder a las consultas planteadas por los responsables de los ficheros sobre las dudas que le planteen, con el fin de interpretar determinados hechos o cuestiones que no tienen una redacción muy clara dentro de la normativa sobre protección de datos.

La forma que tiene la AEPD de responder a estas consultas es a través de informes jurídicos, que aunque carecen de carácter vinculante, sí que pueden ayudar a conocer la postura de la Agencia en relación a determinadas cuestiones de interés.

7.3.1 Ámbito de aplicación

Procedimiento E-00561-2004 e Informe 669-2009: Consideración del DNI como dato de carácter personal

La AEPD en determinadas ocasiones puede cambiar de criterio, y considerar en un principio que determinados datos deben quedar fuera del ámbito de aplicación de la normativa sobre protección datos, para posteriormente cambiar de postura, e incluirlos dentro del ámbito.

El caso más significativo en este aspecto fue el relativo al DNI. En un principio, la AEPD consideraba que el número de DNI, por sí sólo, no era un dato de carácter personal, y que para ser considerado como tal debía ir adscrito al concreto titular del mismo, para hacer a esa persona, identificada e identificable.

Sin embargo con la entrada en vigor del RLOPD, la AEPD cambió, con buen criterio, la consideración del DNI como dato de carácter personal en base a los siguientes criterios:

- El RLOPD define como persona identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.

  Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

- El Real Decreto 1553/2005, de 23 diciembre concede al DNI un valor suficiente, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, debido a que a cada DNI se le asigna un número personal que tendrá la consideración de identificador numérico personal de carácter general.

7.3.2 Consentimiento

Informe 0352 - 2009: Solicitud de consentimiento para envío de publicidad de terceros

En este informe se indica es la necesidad que existe de solicitar de consentimiento para envío de publicidad de terceros.

Determina que para que la cláusula en la que se solicita el consentimiento para el envío de publicidad a través de cualquier medio deberá precisar los sectores específicos y concretos de la actividad a que va a referirse dicha publicidad.

Dicha cláusula tendrá un carácter vinculante para el responsable del fichero, de forma que si se necesitara realizar un nuevo tratamiento de los datos con fines publicitarios para un sector diferente de aquellos fijados en ella, se necesitará de un nuevo consentimiento del afectado para que éste sea lícito.

Además, se recuerda al responsable del fichero las obligaciones que deberá tener en cuenta a la hora de realizar un tratamiento con fines comerciales:

a) La obligación de informar al afectado sobre la existencia de ficheros comunes de exclusión generales o sectoriales cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial.

b) Consultar previamente los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Informe 0046 - 2010: Tratamiento de datos de menores. Consentimiento y deber de información

El RLOPD regula cómo deberá ser el tratamiento de los datos de los menores de edad, tanto a la hora de prestar el consentimiento como a la hora de informarles sobre sus datos.

Sobre el consentimiento se establece como edad límite, para necesitar otorgarlo o no, los 14 años. Si es menor de 14 años o incapaz, el consentimiento deberá ser otorgado por sus padres o tutores. En relación a la forma de informar, el RLOPD establece que deberá realizarse en un lenguaje que sea ser fácilmente comprensible.

7.3.3 Cesión de datos

Informe 0517 - 2010: Sistemas Institucionales de Protección. Cesiones de datos para la prevención del blanqueo de capitales

En este informe jurídico, se plantea cuál es el régimen jurídico aplicable a las cesiones de datos en el seno de los Sistemas Institucionales de Protección, de un grupo de entidades financieras que constituya un grupo consolidable de entidades de crédito, para

el cumplimiento de las obligaciones de prevención del blanqueo de capitales y de la financiación del terrorismo establecidas en la Ley 10/2010, de 28 de abril, a raíz de lo dispuesto en la normativa sobre protección de datos.

La AEPD considera en este caso que dichas cesiones se realizan con finalidad de prevenir del blanqueo de capitales y la financiación del terrorismo y por lo tanto se encuentran amparada en las excepciones que establece el artículo 11.2 a) de la LOPD.

Informe 0411- 2010: Comunicación de datos de accidentes de tráfico a compañías aseguradoras

En este informe jurídico, la AEPD considera que, no será preciso el consentimiento de los interesados para que puedan cederse los datos relativos a los accidentes de tráfico por la policía local a las compañías aseguradoras.

Para ello se sustenta en que la Ley 50/1980 del Contrato de Seguro y, en la actualidad, el Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados, que deroga la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de seguros privados, ampararían la cesión no consentida, tal y como dispone 11.2.a) de la LOPD, en cuanto que dichas compañías deben recabar y conservar la información necesaria en relación con la indemnización que debe abonarse a terceros como consecuencia de un seguro de responsabilidad civil. Sin embargo, esta comunicación deberá limitarse a los datos que sean necesarios, en cada caso, en relación con las finalidades que justifiquen y habiliten dicha comunicación.

El informe también habilita la utilización del correo electrónico como medio de recepción y de remisión de la documentación solicitada por las compañías aseguradoras, siempre y cuando se cumpla con dispuesto en el artículo 27 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en concreto deberá:

a) Existir una constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique fidedignamente al remitente y al destinatario de las mismas.
b) Haber sido así habilitado como tal por el Organismo en el que presta servicios el consultante.

Informe 0437 - 2010: Dato de correo electrónico de empresa de los trabajadores. Cesión a sindicatos

En este informe jurídico, la postura de la AEPD va a chocar primero con lo establecido en el artículo 2.2 del RLOPD y segundo con la postura emitida en otros informes emitidos sobre el ámbito de aplicación de la normativa sobre protección de datos.

En este informe la AEPD considera que "la dirección de correo electrónico, e-mail profesional, de empresa o corporativo de los trabajadores es un dato de carácter personal el correo electrónico".

Esta consideración se basa en un informe de fecha 15 de noviembre de 2005, emitido con anterioridad a la entrada en vigor del RLOPD, en el que se incluía dentro del ámbito de aplicación de la normativa sobre protección de datos incluido los datos pertenecientes a las personas físicas relativos a: nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

Sin embrago, con la entrada en vigor del RLOPD, y en concreto del artículo 2.2, esta apreciación ha cambiado radicalmente, y dichos datos ya no pueden ser considerados como datos de carácter personal siempre y cuando vayan asociados a personas físicas que presten sus servicios a personas jurídicas.

Lo que sí es significativo es que el presente informe que se analiza es del año 2010, fecha en la cual ya había entrado en vigor el RLOPD, y la misma AEPD, como se apunta anteriormente, había emitido varios informes aclarando esta misma apreciación (Informes jurídicos 78-2008 y 234-2008).

Por lo tanto, la AEPD considera que habrá que analizar cada caso en concreto, para saber, si el correo pertenece a la esfera íntima y personal de una persona física, y como tal debe ser considerado como un dato de carácter personal; o si por el contrario pertenece al individuo dentro de una relación profesional, con lo cual el correo no podrá ser considerado como un dato de carácter personal y quedará fuera del ámbito de aplicación de la normativa sobre protección de datos.

7.3.4 Medidas de Seguridad

Informe 0191 - 2010: Plazo de conservación de informes de Auditoría

En dicho informe la AEPD indica el plazo de conservación del Informe de Auditoría de las medidas de Seguridad.

Se indica que se deberá mantener 2 años de antigüedad del informe.

Informe 0008 - 2010: Fichero de empleados. Medidas de seguridad nivel básico o medio

En dicho informe la AEPD indica que, en caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

- Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
- Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Por ello, respecto de los datos relativos a la minusvalía que son datos relativos a la salud, lo único que se permite es adoptar medidas de seguridad de nivel básico en cuanto a dicho dato se encuentre afectado o vinculado al cumplimiento de deberes públicos, como sería el supuesto del fichero de nóminas en el que aparezca un porcentaje de minusvalía para calcular el nivel de retención aplicable en nómina, conforme a lo previsto en el artículo 103.1 del Real Decreto Legislativo 3/2004, de 5 de marzo por el que se aprueba el Texto Refundido del Impuesto sobre la Renta de las Personas Físicas.

Si por el contrario, el dato de minusvalía se tratara para cuestiones que no constituyan el cumplimiento de deberes públicos, sí deberán de adaptarse medidas de seguridad de nivel alto.

Informe 0487 - 2009: Perfil de comprador de usuario de páginas web. Medidas de Seguridad de nivel medio o alto

Este informe jurídico indica que todos los ficheros que contengan datos a partir de los cuales puedan deducirse cualquiera de las facetas antes mencionadas, como sucede en el presente caso, que incluyen datos relativos al gusto y aficiones que permiten deducir un perfil de los usuarios de las web de la consultante, de modo que el nivel de medidas de seguridad aplicable al supuesto consultado será el medio, debiendo también aplicarse las medidas de nivel básico, toda vez que los niveles son acumulativos.

El informe indica que, si el fichero tuviera datos referentes al perfil psicológico de los afectados habrá de considerarse que el fichero contiene datos relacionados con la salud de las personas, siendo entonces de aplicación las medidas de seguridad de nivel alto, además de las medidas de nivel básico y medio.

Informe 0623 - 2009: Adoptar distintas medidas de seguridad según los ficheros

En este informe jurídico la AEPD, y a raíz de la excepción contenida en el artículo 81 del RLOPD, modificó su criterio inicial de aplicar las medidas de nivel alto a los llamados ficheros de gestión de recursos humanos rebajando las medidas de seguridad aplicables, en los casos establecidos, a nivel básico.

Sin embargo con respecto a los ficheros en los que consten currículos de candidatos, la AEPD considera que las medidas de seguridad que deben aplicarse son las de nivel medio, ya que pueden contener datos que dado que de los datos incluidos en los currículos pueden deducirse hábitos, aficiones de los afectados, se pueden crear perfiles de los mismos, con lo que las medidas de seguridad adoptar son de nivel medio.

7.3.5 Plazo de conservación de datos personales

Informes 0191-2010 y 0408-2010.

En estos informes se recogen las principales dudas que existen a la hora de cancelar los datos de carácter personal es cuánto tiempo debo conservarlos antes de suprimirlos una vez finalizada la necesidad para la que fueron recabados.

La AEPD se remite para solventar esta cuestión al plazo máximo de prescripción de las infracciones que se establece en el artículo 47 de la LOPD, es decir, 3 años.

Por lo que se deberá conservar la documentación como mínimo durante 3 años, sin perjuicio de que deban conservarse por un período superior en caso de que otra norma así lo requiera.

En el caso de los informes de auditoría de seguridad, la AEPD establece una excepción, al considerar que el plazo máximo de conservación de estos informes es de 2 años, período en el que el responsable del fichero deberá mantener dicho informe a disposición de la AEPD.

7.3.6 Cookies

Informe 0196 - 2014: Contenido de la información de la segunda capa en cookies

En esta consulta está referida al cumplimiento del deber de información respecto del uso de tales dispositivos. Se plantea el deber de información por capas, en una primera capa se mostraría la información esencial sobre la existencia de cookies, si son propias o de terceros y las finalidades de las cookies empleadas, así como los modos de prestar el consentimiento y la información sobre un procedimiento de rechazo de cookies.

En una segunda capa a la que se accede mediante enlace o hipervínculo de la primera se ofrecería información adicional sobre las cookies. Esta capa debe tener información sobre qué son y para qué se utilizan las cookies, los tipos utilizados y su finalidad, así como la forma de desactivar o eliminar las cookies a través de las funcionalidades facilitadas, las herramientas proporcionadas por el navegador o el terminal o través de las plataformas comunes que pudieran existir, para esta finalidad, y la forma de revocación del consentimiento ya prestado.

Adicionalmente, en esta segunda capa debe proporcionarse información sobre la identificación de quién utiliza las cookies, si la información es tratada solo por el responsable y/o también por terceros contratados.

7.3.7 Otras cuestiones de interés

Informe 494 - 2008: Necesidad de contrato de encargado de tratamiento con la central

En este caso es importante señalar que para la AEPD, la existencia de un grupo de empresas no afecta para que cada una de las sociedades integradas en el mismo no mantenga diferenciada y plena su personalidad jurídica.

Por este motivo, para la AEPD cada una de las empresas que integran el grupo será responsable del fichero de datos de sus correspondientes empleados.

En consecuencia, cada empresa deberá proceder a notificar de manera independiente sus propios ficheros y cualquier acceso a los datos entre las diferentes sociedades que componen el grupo constituiría un supuesto de cesión que requeriría el consentimiento del afectado o la habilitación legal para la misma.

Para evitar esta cesión es necesario firmar un contrato de encargo de tratamiento adecuado a lo que establece la normativa sobre protección de datos, entre la empresa central del grupo y sus filiales.

Informe 0361 - 2010: Acreditación del cumplimiento del deber de información

Este deber de acreditar, por parte del responsable del fichero, que se ha cumplido con el deber de información venía regulado en el artículo 18 del RLOPD, si bien la Sentencia de 15 de julio de 2010, de la Sala Tercera del Tribunal Supremo, ha anulado dicho precepto al considerar que contravenía la LOPD.

Según esta Sentencia debe prevalecer la libertad de forma tanto para la prueba de la obtención del consentimiento del interesado, como para la acreditación del cumplimiento del deber de información al mismo, por lo que no se pueden establecer obligaciones adicionales al margen de lo que establece la normativa sobre protección de datos.

Sin embrago, este informe sí que permite como un medio válido y apropiado de prueba para acreditar el haber cumplido con el principio de información, la sustitución de los documentos originales en papel por un soporte informático mediante el escaneado de los mismos, siempre y cuando se garantice que en dicha automatización no ha mediado alteración alguna de los soportes originales.

Para ello, los responsables del fichero deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal que se establecen en la normativa sobre protección de datos, dejándoles libertad a para elegir la utilización de medios técnicos siempre que se consiga el resultado previsto en dicha normativa.

Informe 0464 - 2013: Anexo al contrato de trabajo sobre deber de confidencialidad. Uso de Internet y correo electrónico.

En este informe jurídica se indica que es factible la entrega a todos los trabajadores junto con la nómina de un determinado mes, de un Anexo que en cumplimiento del deber del responsable del fichero de adoptar las medidas necesarias para que el personal que tenga acceso a datos personales conozca su deber de secreto profesional respecto de tales datos, que subsistirá incluso una vez extinta la relación laboral.

En referencia al uso electrónico corporativo, puesto que se reconoce la propiedad empresarial de dicho correo y que el mismo será destinado “para fines profesionales, si bien se autoriza al trabajador a que pueda hacer uso de dichas herramientas de trabajo para fines personales, siempre que el mismo se realice de manera razonable y conforme al principio de buena fe contractual”.

Por ello, se indica que la empresa de acuerdo con las exigencias de buena fe, debe establecer previamente las reglas de uso de esos medios e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones.

Capítulo 8

Prototipo para la auditoría de las medidas de seguridad exigidas por el RLOPD

8.1 Descripción general del programa

El programa de Auditoría se ha implementado en Microsoft Excel, de esta forma permite de una manera sencilla verificar el cumplimiento de las medidas de seguridad requeridas por el Reglamento de Desarrollo de la LOPD en el Título VIII.

Para ello, se distribuye en varias pestañas que permiten mantener el detalle de las pruebas a realizar así como el estado de la revisión a llevar a cabo.

Se ha elaborado una conexión con Microsoft Word, de forma que se permite generar el Informe de Auditoría en ese formato para una sencillez en la obtención y manejo de la información.

En las próximas secciones se describirá cada una de las pestañas del Libro Excel para indicar qué realiza cada una de ellas y sus capacidades.

El libro Excel está formado por 3 pestañas:

- Pestaña “Programa de trabajo”, que contendrá el detalle de la revisión que se estará llevando a cabo por el equipo de Auditoría.

- Pestaña “Programa general”, que contiene el detalle de las pruebas que se han definido para garantizar el cumplimiento así como los hechos observados y recomendaciones que se derivan de la no conformidad de la prueba.

- Pestaña “Resumen”, de carácter interno de la aplicación, y que permite obtener la información con el formato requerido.

8.2 Pestaña “Programa de trabajo”

En este apartado se describe el estado de la revisión del cumplimiento de las medidas de seguridad requeridas por el Título VIII del Reglamento de Desarrollo de la LOPD.

Dentro de este apartado se encuentra el detalle de cada una de las pruebas, los hechos observados, así como la existencia de incidencias en el cumplimiento.

Cuando el usuario abra el documento Excel, aparecerá la siguiente pantalla:

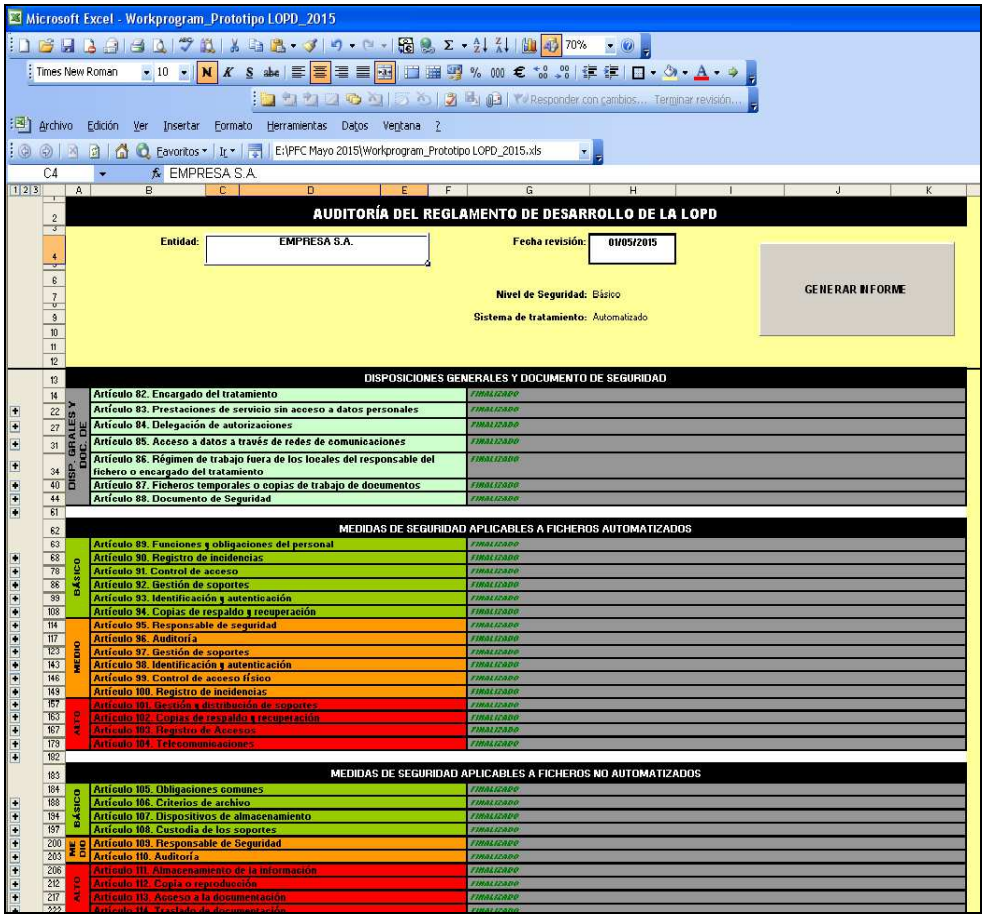


Figura 6: Detalle prototipo: Pestaña principal del seguimiento de la Auditoría

8.2.1 Encabezado

En el encabezado, aparece la siguiente información:

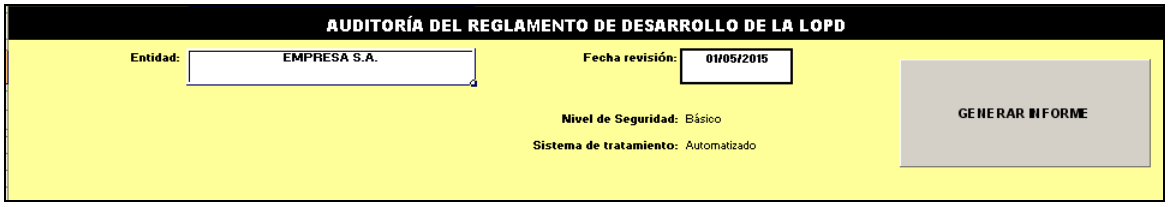


Figura 7: Detalle prototipo: Información general acerca de la Auditoría

El equipo de Auditoría, deberá completar la siguiente información:

- **Entidad**, campo donde se puede incluir el nombre de la Entidad en la que se está realizando la revisión del grado de cumplimiento. Esta información aparecerá en el informe generado automáticamente a partir de la revisión efectuada.

- **Fecha de revisión**, campo donde se puede incluir la fecha correspondiente a la revisión llevada a cabo. Esta información aparecerá en el informe generado automáticamente a partir de la revisión efectuada.

- **Nivel de Seguridad**, campo de selección donde se indicará el nivel de Seguridad a auditar:
  - Básico
  - Medio
  - Alto

- **Sistema de Tratamiento**, campo de selección donde se indicará el tipo de sistema de tratamiento a auditar:
  - Automatizado
  - No Automatizado
  - Mixto

8.2.2 Secciones de medidas de seguridad de nivel básico, medio o alto para ficheros automatizados y no automatizados

Las medidas de seguridad se encuentran agrupadas por:

- **Disposiciones Generales**

DISPOSICIONES GENERALES Y DOCUMENTO DE SEGURIDAD		
DISP. GRALES Y DOC. DE	Artículo 82. Encargado del tratamiento	FINALIZADO
	Artículo 83. Prestaciones de servicio sin acceso a datos personales	FINALIZADO
	Artículo 84. Delegación de autorizaciones	FINALIZADO
	Artículo 85. Acceso a datos a través de redes de comunicaciones	FINALIZADO
	Artículo 86. Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento	FINALIZADO
	Artículo 87. Ficheros temporales o copias de trabajo de documentos	FINALIZADO
	Artículo 88. Documento de Seguridad	FINALIZADO

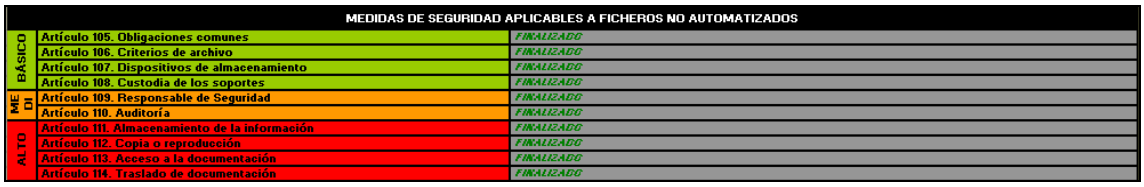
Figura 8: Detalle prototipo: Disposiciones Generales

- **Medidas de Seguridad aplicables a ficheros automatizados**

MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS AUTOMATIZADOS		
BÁSICO	Artículo 89. Funciones y obligaciones del personal	FINALIZADO
	Artículo 90. Registro de incidencias	FINALIZADO
	Artículo 91. Control de acceso	FINALIZADO
	Artículo 92. Gestión de soportes	FINALIZADO
	Artículo 93. Identificación y autenticación	FINALIZADO
	Artículo 94. Copias de respaldo y recuperación	FINALIZADO
MEDIO	Artículo 95. Responsable de seguridad	FINALIZADO
	Artículo 96. Auditoría	FINALIZADO
	Artículo 97. Gestión de soportes	FINALIZADO
	Artículo 98. Identificación y autenticación	FINALIZADO
	Artículo 99. Control de acceso físico	FINALIZADO
	Artículo 100. Registro de incidencias	FINALIZADO
ALTO	Artículo 101. Gestión y distribución de soportes	FINALIZADO
	Artículo 102. Copias de respaldo y recuperación	FINALIZADO
	Artículo 103. Registro de Accesos	FINALIZADO
	Artículo 104. Telecomunicaciones	FINALIZADO

Figura 9: Detalle prototipo: medidas de seguridad ficheros automatizados

- **Medidas de Seguridad aplicables a ficheros no automatizados**



MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS NO AUTOMATIZADOS		
BÁSICO	Artículo 105. Obligaciones comunes	FINALIZADO
	Artículo 106. Criterios de archivo	FINALIZADO
	Artículo 107. Dispositivos de almacenamiento	FINALIZADO
	Artículo 108. Custodia de los soportes	FINALIZADO
MEDIO	Artículo 109. Responsable de Seguridad	FINALIZADO
	Artículo 110. Auditoría	FINALIZADO
ALTO	Artículo 111. Almacenamiento de la información	FINALIZADO
	Artículo 112. Copia o reproducción	FINALIZADO
	Artículo 113. Acceso a la documentación	FINALIZADO
	Artículo 114. Traslado de documentación	FINALIZADO

Figura 10: Detalle prototipo: medidas de seguridad ficheros no automatizados

Cada una de estas secciones se distribuye en los niveles dentro de estas agrupaciones se encuentra el detalle de cada uno de los artículos cuyo análisis será requerido para verificar el grado de cumplimiento.

Se ha utilizado las funcionalidades aportadas por Excel para agrupación de filas, con el fin de aclarar y proporcionar más sencillez.

De esta forma, si el usuario pincha en el símbolo  que se encuentra a la izquierda de la hoja de cálculo, que indica el nivel de agrupación, aparecerá para cada artículo el detalle de pruebas a realizar:

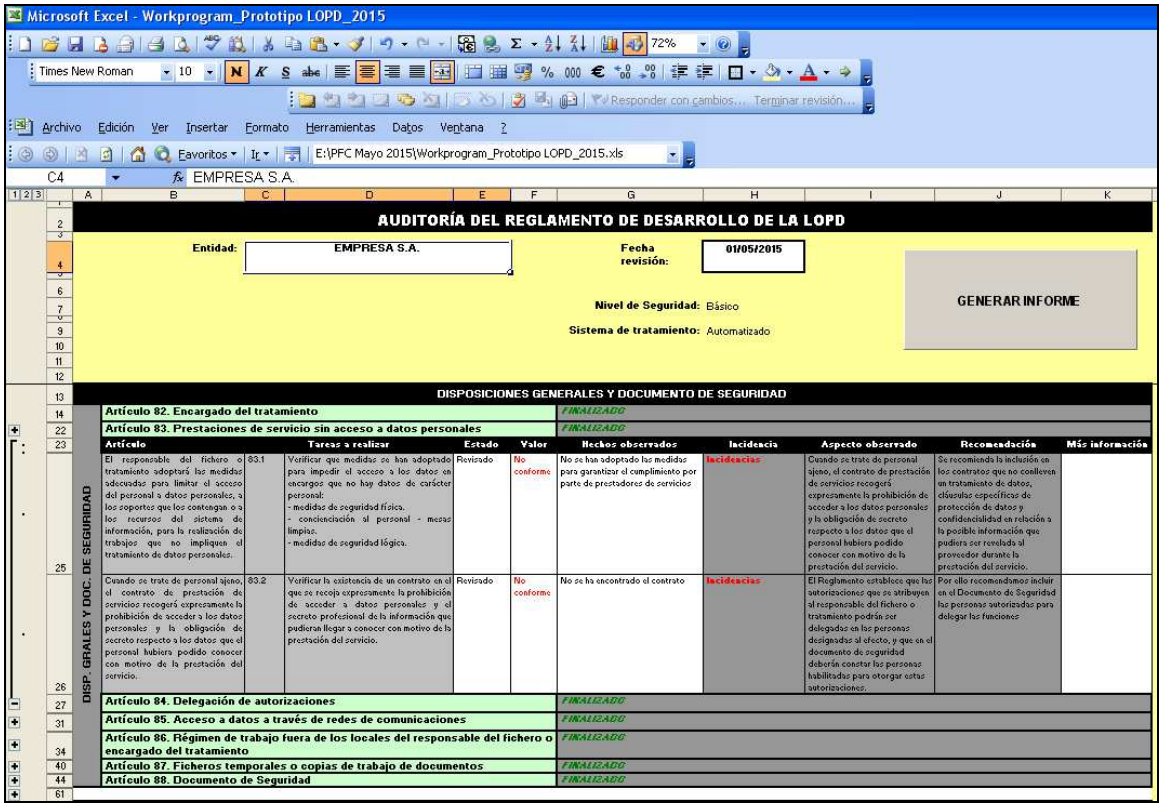


Figura 11: Detalle prototipo: pruebas a realizar para el artículo seleccionado

El detalle de la información recogida es el siguiente:

- **Artículo**, indica el artículo en cuestión y el detalle del mismo.

- Valor **Estado** de la revisión del artículo, será un campo cuyos valores posibles son:

    - Finalizado, si todas las pruebas se han llevado a cabo, apareciendo marcado en color verde para identificar claramente que se ha cerrado este apartado.
    - Pendiente, si alguna de las pruebas está sin concluir, apareciendo marcado en color amarillo.

- **Tareas a realizar**, donde se indica el detalle de pruebas a realizar, dicha información será obtenida del detalle de pruebas que se hayan incluido en “Programa de Trabajo General” para el artículo en cuestión.

- **Estado**, que se corresponde con el estado de la revisión, sus valores posibles son:

    - “Revisado”
    - “No revisado”

- **Valor**, que contempla la valoración resultante del análisis de la prueba de cumplimiento, los valores posibles son:

    - “Conforme”
    - “No conforme”

- **Hechos observados**, campo en el que se puede incluir el detalle y/o resultado de la prueba realizada, información analizada, conclusiones principales obtenidas.

  Es importante tener en cuenta que este campo no se trasladará al Informe de Auditoría, sino que es un área en el que se puede recoger información necesario para la valoración de la prueba necesaria para el desarrollo del trabajo de campo.

- **Incidencia**, campo que recoge el resultado del análisis de la prueba de cumplimiento, los valores posibles son:

    - “Incidencias”
    - “Sin incidencias”

- **Aspecto observado**, campo que recoge el hecho observado tras la realización y análisis de la prueba de cumplimiento, los valores posibles son:

    - En blanco, si no existen incidencias.
    - Detalle del hecho observado, si existen incidencias.

- **Recomendación**, campo que recoge la recomendación que es necesario establecer tras la realización y análisis de la prueba de cumplimiento, los valores posibles son:

    - En blanco, si no existen incidencias.
    - Detalle del hecho observado, si existen incidencias.

- **Más información**, campo en el que se puede incluir información de texto libre en el caso de que se desee añadir información adicional. Este campo puede ser muy útil para incluir las referencias a las evidencias que dan soporte a la prueba o para incluir cualquier otro tipo de información adicional.

De igual, forma, si el usuario pincha en el símbolo [-], se agruparán las pruebas del artículo correspondiente.

Siguiendo las opciones propias de Microsoft Excel se podrán agrupar o desagrupar toda la información.

8.3 Pestaña Programa de trabajo general

En este apartado se describe un modelo de programa de trabajo para realizar la revisión de la implementación de las medidas de seguridad requeridas por el Título VIII del Reglamento de Desarrollo de la LOPD.

El programa de Auditoría propuesto se incluye dentro de la pestaña etiquetada como "*PROGRAMA GRAL*".

Es en este apartado donde se incluye el detalle de las pruebas que proponemos que habría que realizar para poder determinar el grado de cumplimiento, las pruebas aquí detalladas son las que se han ido comentando a lo largo de todas las secciones que contempla este documento.

Artículo	Descripción	Código Prueba	Prueba	Observación	Recomendación	Criticidad
Artículo 82. Encargado del tratamiento	1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.	82.1	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los locales del responsable del fichero, se incluye esta información en el documento de seguridad.	El Reglamento establece que cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.	Por ello recomendamos incluir estos aspectos en el Documento de Seguridad.	Alta
		82.2	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los locales del responsable del fichero, existe un contrato/compromiso de confidencialidad firmado por parte del personal del encargado del tratamiento en cumplimiento de las medidas de seguridad.	El Reglamento establece que cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.	Por ello recomendamos establecer un procedimiento de compromiso para el personal del encargado del tratamiento en cumplimiento con las medidas de seguridad.	Alta
	2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.	82.3	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los propios locales del encargado del tratamiento, se incluye esta información en el documento de seguridad.	El Reglamento establece que cuando el acceso por parte del encargado del tratamiento sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.	Por ello recomendamos incluir estos aspectos en el Documento de Seguridad.	Alta
		82.4	Verificar que, en el caso de que exista un encargado del tratamiento ubicado en los propios locales del encargado del tratamiento, existe un contrato/compromiso de confidencialidad firmado por parte del personal del encargado del tratamiento en cumplimiento de las medidas de seguridad.	El Reglamento establece que cuando el acceso por parte del encargado del tratamiento sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.	Por ello recomendamos establecer un procedimiento de compromiso para el personal del encargado del tratamiento en cumplimiento con las medidas de seguridad.	Alta
		82.5	Verificar la existencia de un documento de seguridad del encargado del tratamiento que verifique que éste posee identificado el fichero y que implementa las medidas de seguridad requeridas.	El Reglamento establece que si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.	Por ello recomendamos solicitar al encargado del tratamiento el documento que justifique que éste ha identificado el fichero y que posee un documento de seguridad en el que se recogen las medidas de seguridad a implantar.	Alta
	3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.	82.6	Verificar la existencia de un documento en el que se establezca el compromiso por parte del encargado del tratamiento para la implantación de las medidas de seguridad.	El Reglamento establece que el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este Reglamento.	Por ello recomendamos solicitar al encargado del tratamiento el documento que justifique el cumplimiento de las medidas de seguridad requeridas.	Alta
Artículo 83. Prestaciones de servicio sin acceso a datos personales	El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.	83.1	Verificar que medidas se han adoptado para impedir el acceso a los datos en encargos que no hay datos de carácter personal: - medidas de seguridad física. - concienciación al personal - mesas limpias. - medidas de seguridad lógica.	El Reglamento establece que el responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.	Por ello recomendamos implantar determinadas medidas para prevenir el acceso a información, soportes o recursos a personal que se encuentre en las instalaciones para la realización de trabajos que no impliquen tratamiento de datos personales. Es recomendable la implantación de: - sistemas de control de acceso físico a los recursos, equipos informáticos. - concienciación al personal sobre la custodia de información en papel. - mecanismos de acceso lógico para prevenir el acceso a los sistemas de información.	Alta
	Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.	83.2	Verificar la existencia de un contrato en el que se recoja expresamente la prohibición de acceder a datos personales y el secreto profesional de la información que pudieran llegar a conocer con motivo de la prestación del servicio.	Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.	Se recomienda la inclusión en los contratos que no conlleven un tratamiento de datos, cláusulas específicas de protección de datos y confidencialidad en relación a la posible información que pudiera ser revelada al proveedor durante la prestación del servicio.	Alta

Figura 12: Detalle prototipo: Pruebas incluidas

Se compone de la siguiente información:

- **Artículo**, donde se recoge el artículo del RLOPD correspondiente y el detalle del mismo para que el auditor siempre disponga de esta referencia.

- **Código Prueba**, donde se define un código de la prueba para poder ser referenciada claramente.

- **Prueba**, referido al detalle de la prueba a llevar a cabo que verifique el cumplimiento del artículo correspondiente.

- **Observación**, donde se incluye el hecho observado que se detecta en el caso de que el resultado de la prueba resulte que no existe un cumplimiento del artículo y que por lo tanto, sea necesario trasladar dicha incidencia en el Informe de Auditoría.

- **Recomendación**, donde se detalla la recomendación resultante del incumplimiento de la medida requerida y que aparecerá en el Informe de Auditoría.

- **Criticidad**, que recoge el nivel de criticidad a la recomendación en cuestión.

8.4 Acciones que puede realizar el usuario

8.4.1 Cómo puede el usuario modificar el programa de trabajo

El equipo de Auditoría puede modificar del programa de trabajo la siguiente información:

- Campo **Prueba**, si el usuario desea modificar el detalle de la prueba a realizar, para ello, accederá a la pestaña de "*PROGRAMA GRAL*" y podrá modificar el detalle de la prueba a realizar.

- Campo **Observación**, si el usuario desea modificar la observación que aparecerá en el Informe en el caso de que la prueba no sea Satisfactoria y por tanto, aparezca un incumplimiento, se accederá a la pestaña de "*PROGRAMA GRAL*" y se podrá modificar el texto que aparecerá.

- Campo **Recomendación**, si el usuario desea modificar la recomendación que aparecerá en el Informe en el caso de que la prueba no sea Satisfactoria y por tanto, aparezca un incumplimiento, se accederá a la pestaña de "*PROGRAMA GRAL*" y se podrá modificar el texto que aparecerá.

- Campo **Criticidad**, si el usuario desea modificar la criticidad con la que se identificará la incidencia, y que aparecerá en el Informe, se accederá a la pestaña de "*PROGRAMA GRAL*" y se podrá modificar el texto que aparecerá.

8.5 Informe de Auditoría

Una vez que el equipo de Auditoría haya realizado las pruebas de auditoría incluidas en el programa de trabajo podrá generar un informe de Auditoría.

El prototipo se ha diseñado en Microsoft Word por su sencillez y versatilidad.

El informe que se genera obtiene por cada uno de los artículos las pruebas realizadas y si su valoración tiene incidencias o no, en el caso de que existan incidencias se mostrará:

- Hecho observado
- Incidencia detectada
- Recomendación propuesta

8.5.1 Cómo generar el Informe de Auditoría

Para obtener un informe de la Auditoría llevada a cabo en la Entidad, únicamente deberá pinchar el botón cuyo nombre es "Generar informe" que se encuentra en la pestaña de "*PROGRAMA DE TRABAJO*".

A continuación, a través de un desarrollo en Visual Basic facilitado por Excel, el programa irá obteniendo la información recogida en cada una de las pruebas y volcando esta información con el formato establecido en un Documento Word.

Al final de la obtención de información aparecerá un mensaje en pantalla, avisando de esta forma al usuario de que el volcado de datos ha finalizado:

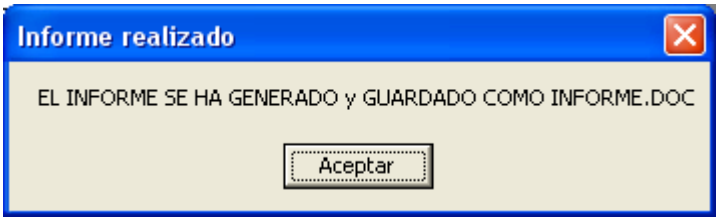


Figura 13: Pantalla Informe generado

El Informe se guardará automáticamente en la carpeta de *Mis documentos* del equipo informático en el que se esté ejecutando, con el nombre de "***Informe.doc***"

AUDITORIA DE CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD RLOPD

EMPRESA S.A.

Fecha de revisión: 01/05/2015

Artículo 82. Encargado del tratamiento - Prueba 1

Sin incidencias

Artículo 82. Encargado del tratamiento - Prueba 2

Sin incidencias

Artículo 82. Encargado del tratamiento - Prueba 3

Incidencias

Hecho observado
No se recoge en el documento de seguridad los encargos de tratamiento en las instalaciones del proveedor

El Reglamento establece que cuando el acceso por parte del encargado del tratamiento sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Recomendación
Por ello recomendamos incluir estos aspectos en el Documento de Seguridad.

Criticidad:
Alta

Artículo 82. Encargado del tratamiento - Prueba 4

Sin incidencias

Artículo 82. Encargado del tratamiento - Prueba 5

Sin incidencias

Figura 14: Ejemplo Informe de Auditoría generado

El equipo de Auditoría, podrá modificar este archivo en formato Word, proporcionándole el formato que sea requerido o agregando alguna otra información que sea necesaria.

Capítulo 9

Nuevos retos de la protección de datos

9.1 El Derecho al olvido en Internet

El “derecho al olvido” en Internet se ha erigido en uno de los más intensos temas de debate en el entorno de los nuevos servicios de Internet, al amparar la capacidad de una persona para borrar de Internet información irrelevante sobre sí misma y preservar de este modo su privacidad.

Reconoce la cancelación de un dato personal que se ha recabado legítimamente para que se retire cuando se agote la finalidad para la que fue obtenido.

Supone, por tanto, la pretensión legítima de un particular de borrar los datos que hacen referencia a su persona en Internet en los casos en los que su aparición en la misma no ha sido por voluntad propia, sino como consecuencia de figurar en un archivo, público o privado, y el motivo de ello carezca de interés público.

Sin embargo, esta pretensión decaería si se trata de un hecho de interés público (aparecer en la Red como autor de un delito por el que fue condenado por sentencia firme).

Este derecho significa, por tanto, hacer realidad el poder de cualquier ciudadano a disponer de toda la información de la que es titular, y a que la memoria digital no se convierta en algo perpetuo.

Conscientes de esta problemática, la Comisión Europea ha puesto en marcha un proceso legislativo para reforzar la protección de datos de los ciudadanos y adaptar las viejas normas al entorno virtual, donde los documentos no solo son de alcance global sino también eternos.

La reforma va enfocada a regular el almacenamiento en Internet de datos personales que no son de interés público, así como a hacerlos desaparecer de los buscadores (Google, Yahoo, YouTube,..) o de redes sociales si el interesado lo solicita (Facebook o Tuenti), dotando al usuario del control de sus datos, pudiendo exigir el completo borrado, incluidas fotografías, cuando se den de baja en el servicio.

La UE aspira a dotar de transparencia este translucido mundo digital, instando a que los proveedores de servicios de Internet o los buscadores recojan los mínimos datos de los usuarios (principio de minimización de los datos) y que lo hagan de manera tan clara como para saber quién los almacena, cómo, con qué finalidad y por cuánto tiempo.

Dentro del territorio español los ciudadanos reclaman cada vez con mayor intensidad la posibilidad de ejercer un control sobre sus datos personales incluido el derecho a no figurar en ella, lo que ha originado una creciente demanda de consultas relacionadas sobre cómo desaparecer de Internet y sobre el ejercicio de los derechos de cancelación y oposición en la AEPD.

El origen de estas reclamaciones se encuentra en la publicación de datos personales en boletines y diarios oficiales, medios de comunicaciones digitales, sentencias y otros sitios web.

De este modo la AEPD ha dado respuesta a las demandas de los ciudadanos en servicios prestados por empresas multinacionales por considerar que para ello utilizan medios en territorio español y se dirigen específicamente a usuarios radicados en España.

Parte de las resoluciones han sido recurridas ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional estando pendiente de dictarse las primeras sentencias que, sin duda, constituirán un novedoso precedente sobre la protección de datos en Internet.

9.2 Tecnología RFID

La identificación por radio frecuencia o RFID (Radio Frequency Identification) es una tecnología que permite identificar automáticamente un objeto gracias a una onda emisora incorporada en el mismo que transmite por radiofrecuencia los datos identificativos del objeto, siendo una identificación normalmente unívoca.

La etiqueta RFID permite almacenar y enviar información a un lector a través de ondas de radio.

Estas etiquetas se caracterizan por ser pequeñas y en la actualidad se implementan a través de pequeños adhesivos que se pueden incorporar prácticamente a cualquier objeto.

El objeto que lleva adherido una etiqueta RFID puede ser localizado a una distancia variable. Un lector físico se encarga de recibir esta señal, transformarla en datos y transmitirla a la aplicación que gestiona esta información.

La tecnología RFID está utilizada principalmente:

- Identificación unívoca de productos, sector logístico, almacenamiento y distribución.
- Sistemas de pago: peajes, transporte.
- Como mecanismos de protección de productos anti robo.

La tecnología RFID presenta nuevas oportunidades así como una mayor eficiencia en determinados sistemas de gestión de uso diario.

Desde la perspectiva del cumplimiento normativo en la utilización de la tecnología RFID, se debe tener en cuenta los riesgos que de la misma se derivan para la seguridad de la información y la privacidad de las personas.

En ocasiones, la información obtenida podrá ser susceptible de contener datos de carácter personal (por ejemplo datos identificativos del nombre y apellidos, datos de salud, gustos, hábitos de consumo, etc.) de aquellas personas que las utilicen, así como obtener datos de geolocalización, de forma que será preciso que las empresas que utilicen productos con tecnología RFID realicen un tratamiento de datos personales, e implementen los mecanismos establecidos por los dictámenes y recomendaciones emanadas de las autoridades europeas en la materia.

Se establecen determinadas recomendaciones que deberán implantarse por aquellas entidades que recaben datos de carácter personal mediante dicha tecnología, entre las que destacan las siguientes:

- Es de aplicación el artículo 4 de la LOPD, definir claramente las finalidades y uso de la información, que deben ser proporcionadas a las finalidades perseguidas.

- Se deberá informar previamente al sujeto del tratamiento de sus datos, en los términos del artículo 5 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, en adelante LOPD. Adicionalmente a todos los aspectos requeridos por el Artículo 5.1 de la LOPD se tienen que tener en cuenta otros aspectos tales como:

    - Indicar el uso de las etiquetas a través de información clara y en un lugar visible.
    - Debe indicar el modo de desactivar las etiquetas o extracción de las mismas.

- Se deberá adoptar los procedimientos necesarios para posibilitar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento.

- Se deberá garantizar las medidas de seguridad establecidas en el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en función de la tipología de los datos recabados en las etiquetas.

Por su parte, el Grupo de Trabajo del Artículo 29 determina en su Dictamen 9/2011 relativo a la Propuesta Revisada de la Industria para un Marco de Evaluación del Impacto sobre la Protección de Datos y la Intimidad en las Aplicaciones Basadas en la Identificación por Radiofrecuencia (RFID), de 11 de febrero de 2011, el impacto de las aplicaciones basadas en la identificación por radiofrecuencia, promoviendo la necesidad de establecer por parte de los operadores RFID, un Informe de Evaluación de Impacto.

De forma que toda empresa que emplee para la recogida y tratamiento de datos de carácter personal tecnología basada en RFID, deberá garantizar el cumplimiento establecido por dicho Informe antes de proceder a la ejecución y/o desarrollo de la aplicación.

El mencionado Informe deberá estar disponible a requerimiento de la Autoridad de Control de cada estado miembro, por lo que el órgano competente en España será la AEPD.

En consecuencia, el incremento en la utilización de la tecnología RFID por parte de las empresas supone que deberán actuar conforme al marco de regulación establecido, de manera que los derechos de la privacidad, intimidad y protección de datos de las personas no se encuentren amenazados.

9.3 Cloud Computing

El término “Cloud Computing” hace referencia a un nuevo modelo de prestación de servicios de tecnología en el que todos los recursos de información pueden ser almacenados en servidores de terceros y accesibles a través de Internet.

Los proveedores disponen de centros de procesos de datos para dar servicio a múltiples usuarios, las compañías clientes reciben un soporte flexible a sus necesidades y particularidades de su actividad en cada momento.

Desde los últimos años, si vienen ofreciendo este tipo de prestación de servicios que se establecen como alternativas más dinámicas y un menor coste que los servicios tradicionales, si bien, es necesario tener en cuenta que es una evolución de las diferentes modalidades de externalización del servicio que ya funcionaban en la actualidad.

Dependiendo del tipo de servicio contratado, la compañía cliente delega la gestión y control de la infraestructura, la red de comunicaciones, los servidores, los sistemas operativos, el almacenamiento e, incluso, las aplicaciones, en una tercera parte mediante la contratación de los servicios acordados.

Dentro de este apartado, vamos a explicar:

- Tipología de servicios
- Modelos de servicios existentes, incluyendo para cada uno las ventajas y riesgos generales que pueden conllevar.
- Riesgos desde el punto de vista del cumplimiento normativo.

9.3.1 Tipos

Existen diferentes tipos de computación en la nube:

- **Nubes públicas:**
  Son aquellas que son administradas por el proveedor del servicio, de esta forma, el control de los recursos, procesos y datos están en manos de terceros.
  No requieren de una inversión inicial por parte de la compañía cliente para comenzar a utilizarlas, ni suponen un gasto de mantenimiento.

  Estas nubes están a disposición del público general, son compartidas con otras compañías clientes dentro de los centros de proceso de datos del proveedor, siendo propiedad de la organización que ofrece los servicios de computación en la nube. El coste asociado al uso suele ser relativamente bajo, lo que las hace atractivas.

- **Nubes privadas:**
  Las nubes privadas son administradas por la compañía cliente para obtener un mayor control. De esta forma, se gestiona únicamente para una organización.

  Debido a esto, supone una inversión inicial en la infraestructura ya que ésta será alojada en las instalaciones de la compañía. De esta forma, la compañía cliente disfruta de una nube de su propiedad donde él es el único que reside en ella, supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, aunque los gastos de mantenimiento corren a cuenta del propietario.

- **Nubes híbridas:**
  Se trata de una opción intermedia, la idea principal consiste en que la compañía cliente podrá mantener el control de aquellas aplicaciones principales y delegar la administración en las que considere secundarias.

  Se trata de dos o más nubes que se mantienen como entidades separadas pero que están unidas por tecnología que permite la portabilidad de datos y aplicaciones, esta solución disminuye la complejidad y coste de la nube privada.

- **Nubes comunitarias:**
  La infraestructura de esta nube es compartida por varias organizaciones, que forman una comunidad con principios similares (normativas específicas de seguridad, sectorial, cumplimientos normativos). Puede ser administrada por la

comunidad o por un tercero. Este modelo puede ser visto como una variación en el modelo de nube privada.

9.3.2 Modelos de servicio de "Cloud Computing"

9.3.2.1 Infraestructura como servicio (IaaS, Infrastructure as a Service)

Este modelo de servicio consiste en una infraestructura de procesamiento completa. El cliente dispone de una o varias máquinas virtuales en la nube.

La capacidad suministrada a la compañía cliente es la posibilidad de abastecerse de procesamiento, almacenamiento, redes y otros recursos computacionales fundamentales de forma que el consumidor pueda desplegar y ejecutar software, que puede incluir sistemas operativos y aplicaciones.

La compañía cliente no gestiona ni controla la infraestructura de la nube pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y la posibilidad de tener un control limitado de componentes de red seleccionados.

Ventajas:

- Transparencia para el usuario. Los usuarios no deben tener ningún conocimiento sobre la infraestructura que soporta el software.
- Sin fuerte inversión inicial. Sólo requiere de pagos mensuales sin la necesidad de pagar el elevado coste del establecimiento de una infraestructura.
- Sin coste de mantenimiento. El coste de mantenimiento de la infraestructura está incluido en el servicio ofrecido por el proveedor.
- Flexibilidad. Simplifica el alineamiento con las necesidades dinámicas de negocio.
- Sin compromiso. Si la solución adoptada no convence al cliente, éste puede cambiar de proveedor y de solución inmediatamente.
- Pago por uso. En ocasiones, las infraestructuras de las compañías están infrautilizadas, suponiendo un coste innecesario. En este modelo, únicamente se incurre en un coste cuando las infraestructuras son utilizadas, evitando así los problemas derivados de mal dimensionamiento.
- Automatización. El hecho de compartir infraestructuras entre varias compañías, supone un alto grado de automatización de procesos estándar, lo que puede ayudar a la eliminación de errores causados por la interacción humana.
- Control. De los tres modelos posibles, IaaS es el que permite mayor control al cliente, pudiendo acceder a los sistemas operativos, gestión de redes y almacenamiento.

Riesgos:

- Errores. El compartimiento de infraestructuras entre compañías de diferentes tipologías y con requerimientos de seguridad diferentes, puede acarrear configuraciones erróneas o insuficientes, exposición de los datos o conductas maliciosas.
- Seguridad a nivel infraestructura. La compañía cliente necesita saber que el proveedor contiene IDS y antivirus en sus sistemas aparte de garantizar que su información no

será vista por otros clientes del mismo proveedor.

- Denegación de servicio. De igual modo, la compañía cliente debe considerar proveedores que estén protegidos ante ataques de denegación de servicio para así garantizar la disponibilidad de su infraestructura.
- Seguridad física. La responsabilidad de garantizar una correcta seguridad física recae sobre el proveedor, ya que las infraestructuras se encuentran en sus instalaciones.
- Dependencia del proveedor. La agilidad del proveedor es crítica en el caso de activación de planes de continuidad de negocio. De igual modo, debe considerarse la forma de desechar los datos por parte del proveedor una vez terminada la relación contractual con el mismo.
- Interrupciones. La disponibilidad máxima que puede alcanzar cualquier servicio online es del 99,9%, lo que implica medio día al año de interrupción en el servicio. La compañía cliente deberá valorar el porcentaje de disponibilidad ofrecido por el proveedor.

9.3.2.2 Plataforma como servicio (PaaS, Platform as a Service)

Es un modelo en el que se ofrece todo lo necesario para soportar el ciclo de vida completo de construcción y puesta en marcha de aplicaciones y servicios web completamente disponibles en Internet. Se encarga de entregar una plataforma de procesamiento completa al cliente sin tener que comprar ni mantener ningún tipo de hardware ni software.

El modelo Platform as a Service proporciona al cliente una plataforma donde poder desplegar las aplicaciones adquiridas o desarrolladas por el mismo, siempre y cuando sean compatibles. El cliente no gestiona ni controla la infraestructura, pero tiene el control sobre las aplicaciones y las configuraciones del entorno del alojamiento de aplicaciones.

Ventajas:

- Simplicidad. En caso de necesitar la implementación en diversas localizaciones o países.
- Disponibilidad total. La plataforma permite ser accedida desde cualquier punto del mundo con conexión a Internet.
- Escalabilidad. Al ser gestionado como un servicio, la plataforma puede ir creciendo de un día para otro en función de las necesidades específicas de cada momento.
- Migraciones simples. Habitualmente se producen mejoras constantes en las plataformas que soportan los sistemas de información, la responsabilidad de mantener las plataformas actualizadas recae sobre el proveedor, debiéndose producir una migración simple y transparente.
- Herramientas de monitorización. Los proveedores de PaaS suelen ofrecer un interfaz que permite la monitorización de la utilización de la plataforma, pudiendo detectar incidencias o nuevas necesidades.
- Reducción de costes en un Plan de Recuperación de Desastres. La naturaleza distribuida del Cloud Computing permite mantener replicada la información en diversas ubicaciones geográficas diferentes, reduciendo así los costes en la gestión de recuperación antes desastres.

Riesgos:

- Inmadurez técnica. Cada entorno en la nube tiene sus propios métodos de interfaz, servicios y costes. Esta inmadurez y la ausencia de criterios comunes puede derivar en empeoramiento o incluso caídas del servicio. Los organismos de estandarización están empezando a estudiar la materia.
- Flexibilidad vs Potencia. Normalmente, el cliente busca más flexibilidad en relación al diseño, desarrollo e implantación para los nuevos sistemas. Sin embargo PaaS no ofrece dicha flexibilidad, su virtud es la oferta de paquetes servicios potentes ya concebidos, no siendo específicos para cada cliente. Esta ausencia de parametrización puede derivar en la contratación de servicios inadecuados.
- Riesgos de cumplimiento legal. Puesto que la responsabilidad de cumplimiento normativo y protección de datos sigue siendo del cliente, deben establecerse contratos entre cliente y proveedor donde se recojan las medidas de seguridad que el segundo debe cumplir.
- Utilización de super-usuarios por parte del prestador de servicios. Se deben analizar especialmente los procedimientos utilizados por parte del proveedor en relación con los usuarios utilizados habitualmente con fines de mantenimiento o seguridad.

9.3.2.3 Software como servicio (SaaS, Software as a Service)

El modelo de Software as a Service consiste en la externalización del mantenimiento, soporte y funcionalidades del software de una compañía.

Podrán existir distintos niveles de servicio dependiendo del grado de personalización; aunque es necesario tener en cuanto que según aumente el grado de personalización también aumentarán los costes.

Ventajas:

- No es necesario comprar, instalar ni mantener el software. Se puede utilizar directamente desde el navegador de Internet.
- Despliegue rápido. Puesto que no es necesaria ninguna instalación, el personal de la compañía puede comenzar a utilizar el servicio desde el día de su contratación.
- Simplicidad. En caso de necesitar el lanzamiento en diversas localizaciones o países.
- Transparencia para el usuario. Los usuarios no deben tener ningún conocimiento sobre la infraestructura que soporta el software.
- Sin fuerte inversión inicial. Sólo requiere de pagos mensuales sin la necesidad de pagar licencias en el momento de la compra.
- Sin instalación de actualizaciones. El proveedor será el encargado de actualizar y mejorar su producto, siendo éste un proceso transparente para el usuario.
- Sin coste de mantenimiento. El coste de mantenimiento del software está incluido en el servicio ofrecido por el proveedor.
- Disponibilidad geográfica total. El sistema permite ser accedido desde cualquier punto del mundo con conexión a Internet.
- Flexibilidad. Simplifica el alineamiento con las necesidades dinámicas de negocio.
- Sin compromiso. Si la solución adoptada no convence al cliente, éste puede cambiar

de proveedor y de solución inmediatamente.
- Libertad de elección. Independientemente del sistema operativo que se utilice, lo único que se necesita es un navegador con acceso a Internet, pudiendo así migrar de plataformas Unix a Windows o Mac con bastante facilidad.

Riesgos:
En referencia a los riesgos generales de este tipo de plataformas, y dado que es el modelo en el que más se delega la seguridad en el proveedor:

- Riesgos de cumplimiento legal.
  La responsabilidad de cumplimiento normativo y protección de datos es de la compañía cliente, por lo que será necesario establecer contratos entre cliente y proveedor donde se recojan las medidas de seguridad que el prestador de servicio debe cumplir, incluyéndose los controles e informes periódicos para que la compañía cliente pueda verificar el cumplimiento de las medidas por parte del prestador.

- Evidenciabilidad.
  El hecho de que la nube sea transparente para el usuario, dificulta la necesidad de evidenciar, ante las autoridades de protección de datos, la correcta implantación de las medidas de seguridad sobre los datos de carácter personal.

- Transferencias Internacionales.
  Es necesario conocer en qué ubicación física se almacenarán los datos de carácter personal; de esta forma es necesario conocer la relación de subcontrataciones que tiene el prestador de servicios, es necesario identificar la relación de transferencias de la información a los distintos países con el fin de detectar y subsanar posibles incumplimientos normativos relativos a las transferencias internacionales de datos.

- Clasificación de la Información: Para proceder con la implantación de las medidas de seguridad apropiadas en función del nivel de los datos de carácter personal, surge la necesidad de clasificar toda la información almacenada en la nube.

- Cifrado y claves: Para el correcto cumplimiento del marco regulatorio existente, es necesario que el proveedor proporcione una adecuada gestión de claves de usuario y permita cifrar las transferencias de datos que así lo requieran.

- Costes ocultos
  Es importante tener en cuenta que existen costes asociados a priori no conocidos, y que pueden surgir asociados al cumplimiento normativo.

- Super usuarios. Se deben analizar especialmente los procedimientos utilizados por parte del proveedor en relación con los usuarios utilizados habitualmente con fines de mantenimiento o seguridad.

9.3.3 Riesgos de cumplimiento normativo

La computación en la nube por su definición trae consigo un conjunto de riegos que deben ser analizados y valorados antes de decidirse por la implementación de una modalidad de computación en la nube.

En este apartado detallamos algunos de los riesgos de incumplimiento normativo que podrían existir.

9.3.3.1 Existencia de un contrato regulado por el artículo 12 de la LOPD

El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio debe regularse en un contrato estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, 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.

En el contrato se deben estipular, asimismo, las medidas de seguridad a que se refiere el RLOPD y que el encargado del tratamiento está obligado a implementar.

Un proveedor de servicios no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del fichero, salvo que se regularice conforme a lo establecido por el artículo 21 del RLOPD.

En base a la normativa española, es necesario una autorización/notificación de la subcontratación en base a la formalización del contrato con el prestador de servicio.

9.3.3.2 Transferencias Internacionales de Datos

La transferencia internacional de datos se define como el tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

La transferencia internacional de datos obliga a distinguir entre los países integrados en el Espacio Económico Europeo frente a estados ajenos a este ámbito geográfico.

9.3.3.3 Copias de respaldo

El modelo seleccionado tendrá que tener en cuenta los aspectos requeridos por la normativa, teniendo que revisar los procedimientos que proporcione el proveedor de Cloud respecto a la realización de copias de respaldo y la verificación periódica cada 6 meses requerida por la normativa de protección de datos.

Es necesario definir una política de respaldo que garantice la recuperación de la información en base a los requisitos de negocio. En base a lo establecido por el Reglamento de Desarrollo de la LOPD, esta copia de seguridad se deberá realizar al menos semanalmente.

La computación en la nube generalmente delega en el proveedor la realización de las copias de respaldo. Será necesario identificar la política de realización de copias de respaldo llevada a cabo por el proveedor verificando que se ajusta a las necesidades de la entidad en base a la criticidad de la información almacenada.

Independientemente de lo anterior, debe tenerse en cuenta que se está delegando en el proveedor la responsabilidad de la realización de las copias de respaldo, por lo que el riesgo de pérdida de información estará ligado a la confianza que se tenga en el proveedor al respecto.

9.3.3.4 Procedimientos de restauración de datos

Es necesario que se defina un procedimiento de restauración de datos en caso de pérdida de información a causa de un error o mal uso de las aplicaciones por parte de algún usuario.

En este sentido, en el caso de servicios de computación en la nube en los que se delega en el proveedor la realización de las copias de respaldo y restauración de los datos, es necesario identificar los procedimientos a seguir para solicitar una restauración de datos y los tiempos de respuesta que el proveedor ofrece al respecto.

Se deberá evaluar si los servicios ofrecidos por el proveedor se ajustan a las necesidades de la compañía en base a la información almacenada.

Por otro lado, es necesario mantener un registro de restauración de datos, que identifique: tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma, las medidas correctoras aplicadas, 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. El proveedor deberá disponer de un registro en que se haya constar toda esta información.

Es necesario definir procedimientos de restauración de datos que identifiquen los canales de solicitud de restauración de datos dentro de la compañía, el personal responsable de su autorización, así como los canales de solicitud con el proveedor.

También hay que tener en cuenta que los tiempos de respuesta ofrecidos por el proveedor estén acordes con las necesidades de negocio.

9.3.3.5 Fuga de información

La computación en la nube ofrece la posibilidad de acceder a los datos desde cualquier lugar en el mundo por medio de una conexión a Internet.

Esta posibilidad es una gran ventaja en cuanto a accesibilidad pero supone también un riesgo para los datos de la compañía, dado que, al ser accesibles desde cualquier lugar, estos datos podrían grabarse localmente en los equipos desde los que son visualizados, independientemente del nivel de seguridad de los mismos.

9.3.3.6 Disponibilidad del servicio

Pese a no tratarse estrictamente de un riesgo de seguridad, sí debe considerarse un riesgo asociado a la disponibilidad del servicio. Es necesario que la Entidad responsable establezca unos determinados niveles de servicio, con el fin de asegurarse que el proveedor de Cloud cumple las necesidades de negocio.

También es importante tener en cuenta que se está delegando en el proveedor la disponibilidad del servicio, confiando en su plan de continuidad de negocio, sus procedimientos de recuperación de desastres que permitan una reacción eficaz ante una grave contingencia.

De esta forma, la Entidad Responsable debería evaluar, cuantificar y mitigar el riesgo asociado a que exista un corte del servicio ofrecido por el proveedor de Cloud.

9.3.3.7 Registro de Acceso a datos de nivel alto

En el caso de que el servicio y/o tratamiento conlleve el tratamiento de datos de carácter personal, habrá que tener en cuenta que se deberán implantar las medidas de seguridad de nivel alto y entre otras, se re requiere de la existencia de un Registro de Acceso.

Este registro debe poder identificar: identificación de usuario, tipo de acceso, fecha y hora de acceso, si el acceso ha sido autorizado o denegado y el registro accedido.

El Registro de acceso debe ser accesible únicamente por el Responsable de Seguridad o las personas que éste designe para realizar las tareas de revisión del Registro de acceso. Es requisito legal realizar una revisión mensual del registro de acceso.

Es necesario que sea posible almacenar el registro de acceso durante al menos un periodo de dos años.

La entidad responsable deberá revisar y analizar cómo se podrá cumplir con este requisito en la infraestructura de Cloud.

9.3.3.8 Capacidad de migración de datos y cancelación del contrato

La prestación de servicio por parte de un Proveedor de Servicios de Cloud, conlleva la utilización de sus propios sistemas de información y/o plataformas, en este sentido, puede crearse una dependencia con el proveedor poco deseada para la entidad cliente de estos servicios que imposibilite la migración de la información a otro proveedor o sistemas internos.

En el caso de que se cancele el contrato con el proveedor de Cloud, sería preciso contar con un procedimiento para recuperar la información alojada por el mismo.

9.3.3.9 Capacidad de auditoría sobre el proveedor

La contratación de servicios de Cloud Computing supone el almacenamiento de información en sistemas ajenos a la compañía, así como la delegación de toda una serie de medidas de seguridad y requerimientos legales en el proveedor del servicio.

No obstante, la Entidad propietaria de los datos sigue siendo responsable sobre los mismos, y deberá velar por que el prestador del servicio reúna las garantías para el cumplimiento de lo dispuesto en el Reglamento.

Es necesario que se establezca por contrato la posibilidad de revisar las medidas de seguridad establecidas por el proveedor, de modo que la compañía pueda revisar en cualquier momento el nivel de cumplimiento respecto a las exigencias legales sobre seguridad de los datos de carácter personal.

Se deberán definir procedimientos específicos de validación de las medidas de seguridad exigidas por contrato al proveedor.

9.3.3.10 Ficheros temporales

Los servicios de Cloud Computing generalmente implican que los datos se encuentren replicados en diferentes máquinas.

No obstante, es requisito legal que las copias de los datos, los ficheros temporales que se creen de forma automática para el correcto funcionamiento de los sistemas, las réplicas de datos por criterios de disponibilidad, etc. cuenten con las mismas medidas de seguridad en todos los casos.

Además, una vez que una copia temporal deje de ser necesaria para la finalidad por la que se ha creado, debe eliminarse de forma que no sea posible su posterior recuperación.

La identificación de todas las copias de la información del Cliente, la seguridad de estas copias así como el borrado seguro de las mismas se encuentra delegada en el proveedor de Cloud.

9.3.3.11 Cifrado de las comunicaciones

En relación a las medidas que debe implementar el Proveedor de Cloud, en referencia a los datos de nivel alto, es necesario tener en cuenta que éstos deberán transmitirse cifrados, por lo que el proveedor de Cloud deberá implantar medidas la utilización de protocolos seguros de comunicación.

9.3.3.12 Borrado seguro de la información

Los servicios de Cloud Computing generalmente implican que los datos se encuentren replicados en diferentes máquinas. El proveedor de Cloud deberá garantizar que la información es borrada de forma segura en todos los sistemas en los que la información se encuentra o se ha encontrado en algún momento de su ciclo de vida. Este hecho se vuelve especialmente relevante ante la finalización de un contrato.

9.3.3.13 Identificación y autenticación de usuarios en los sistemas de información

La Entidad responsable está obligada a garantizar el cumplimiento de estas medidas, independientemente de la subcontratación del servicio. En este sentido, se deberá garantizar:

- Asignar un identificador a cada uno de los usuarios con acceso a la aplicación, que permita relacionar unívocamente el identificador de usuario con la persona física a la que identifica. No se permitirá la utilización de usuarios genéricos ni cuentas grupales.
- Las aplicaciones deben de disponer de diferentes perfiles/roles, dependiendo de las funciones asociadas al tratamiento de datos.
- Los usuarios deberán tener acceso limitado a las funcionalidades requeridas.
- Las aplicaciones permitirán extraer un listado de usuarios con acceso a las aplicaciones y sus distintos perfiles de acceso.
- Las aplicaciones limitarán los usuarios administradores que puedan conceder, alterar o anular el acceso autorizado.
- Se establecerá una caducidad de las contraseñas como máximo de 1 año.
- Las contraseñas deben almacenarse cifradas.
- Establecimiento de una serie de medidas para proporcionar robustez a las contraseñas tales como: implementar una longitud mínima requerida, un histórico de contraseñas con el objetivo de evitar repetir dichas contraseñas, así como la existencia de reglas de complejidad en la composición de contraseñas.
- No se deben permitir un número ilimitado de intentos fallidos de autenticación.
- Obligar al cambio de contraseña tras el primer acceso.
- Habilitar mecanismos de revisión de privilegios y usuarios, así como revisiones de usuarios inactivos.

9.3.3.14 Incidencias no comunicadas por parte del proveedor

El prestador de servicios de Cloud estará obligado a mantener un registro de incidencias que afecten a la seguridad de los datos (en términos de protección de datos, una incidencia se define como cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos).

Este registro de incidencias se requiere en el contrato de prestación de servicio como parte de las medidas de seguridad exigidas al proveedor de Cloud en base a la legislación de protección de datos de carácter personal.

No obstante, no existe a priori obligación legal específica de que el prestador de servicio comunique todas las incidencias periódicamente. Incluso en el supuesto de que así se hiciese, en función del tamaño del proveedor y del tipo de servicio Cloud Computing ofrecido, sería difícil discernir aquellas incidencias que afectasen a información propiedad del Cliente de otros clientes que tengan contratado el servicio con el mismo proveedor de Cloud.

En este sentido, podrían producirse incidencias como ataques cibernéticos, pérdida/robo de servidores, accesos no autorizados, etc. que pudiesen suponer una fuga de información de la Entidad responsable y que ni siquiera se tuviese conocimiento de ello.

9.3.3.15 LSSI

Los prestadores de servicios de la sociedad de la información deben cumplir con los requisitos establecidos en la Ley 34/2002, de servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI).

9.4 Tecnología Big Data

En la actualidad se entiende por Big data el tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que resulta imposible tratarlos con las herramientas de bases de datos y analíticas convencionales.

Dada la proliferación de páginas web, aplicaciones de imagen y vídeo, redes sociales, dispositivos móviles, apps, estos entornos son capaces de generar multitud de información.

La tecnología Big Data, permite analizar dicha información para poder convertirla en información útil para la gestión empresarial:

- Tratamiento de grandes volúmenes de datos.
- Tratamiento de todo tipo de información: de cualquier naturaleza, de cualquier tipología, etc.

- Recogida en cualquier soporte a través cualquier medio.
- Cualquier finalidad en diversidad de sectores.

El Big data permite realizar el tratamiento de grandes volúmenes de información, a través de complejos algoritmos establecer correlaciones e interrelaciones entre los datos de los individuos, obteniéndose conclusiones sobre los mismos. En este sentido, se podría obtener conclusiones y predecir acciones del propio individuo, de esta forma, Big Data permite identificar a un mayor número de clientes potenciales, ofrecerles de forma proactiva nuevos servicios basados en su perfil y retenerles como clientes satisfechos durante más tiempo.

Es importante tener en cuenta que esta tecnología tiene que cumplir con la normativa de protección de datos, por lo que se tendrá que cumplir:

- Principios de transparencia y protección reconocidos por la legislación en materia de protección de datos y que deben conservar el deber de informar, el deber de otorgar consentimiento, finalidades de tratamiento, calidad de los datos, la implantación de las medidas de seguridad correspondientes en función de la tipología de la información, así como la relación de los terceros en los tratamientos.

- Los derechos de los afectados, como elemento esencial para seguir conservando la capacidad para decidir sobre la información que se genera en torno al afectado.

- Principio de calidad de datos y minimización de los datos: datos adecuados y no excesivos.

- Principio de exactitud de datos: posible uso de datos inexactos de fuentes no verificadas.

- Principio de finalidad: uso de los datos con fines legítimos y usos posteriores permitidos.

- Anonimización de datos.

- Privacy by design como marco de diseño básico de toda tecnología que tenga por objetivo el uso o la explotación de datos de carácter personal.

- Adopción de actitud responsable (accountability)

9.5 Internet of the things

Dentro de las nuevas tecnologías que están proliferando se encuentra la denominada Internet of the things, se entiende por esta tecnología la forma de interactuar de dispositivos domésticos tales como: electrodomésticos, relojes, sensores, etc. que envían información vía Internet.

Cabe destacar que a través de estos dispositivos se procesa y envía información del usuario, que puede identificar al usuario, y que puede estar procesando o enviando información relativa tanto a datos identificativos como datos por ejemplo de salud, aficiones, hábitos que permiten obtener una evaluación de la forma de ser del individuo.

Es necesario tener en cuenta que, al tratarse de dispositivos que tratan datos de carácter personal, también tiene que cumplir la normativa de protección de datos, por lo que se deberán cumplir todos los aspectos recogidos en la normativa, de forma especial deberá tenerse en cuenta:

- Se deberá incluir el Deber de Información y recoger el consentimiento del usuario: indicando qué entidad es la responsable del tratamiento de estos datos, qué datos se recogen y para qué finalidades se utilizarán dichos datos.

  Esta información además debe incluirse con total transparencia, de forma que los consumidores estén en todo momento informados acerca del tratamiento y de la localización de sus datos de carácter personal.

- Implantar las medidas de seguridad correspondientes en función del nivel de seguridad de los datos.

  Las medidas de seguridad serán acordes a los aspectos que se han descrito en este proyecto.

- Cancelación de datos
  Será necesario establecer medidas para poder llevar a cabo la cancelación de datos por parte del usuario interesado.

9.6 Nueva regulación europea de protección de datos

Actualmente, se encuentra en borrador la regulación europea acerca de la nueva normativa de protección de datos.

En todo caso, y como aspectos más destacables del borrador de Reglamento, cabe señalar los siguientes:

- Habrá total armonización entre todas las leyes de protección de datos en el futuro, dado el carácter de aplicabilidad directa de esta normativa.

- Existencia de una figura denominada DPO “Data Protection Officer”, que sería un delegado de protección de datos.

  Cabe indicar que en las distintas versiones que se encuentran en modo borrador se ha ido modificando determinados aspectos en relación a la existencia de una figura de

DPO, en lo que se refiere a obligatoriedad, funciones y duración de nombramiento. De esta forma:

- En la propuesta inicial (2012): se establecía que todo ente público o privado con más de 250 empleados, así como entidades cuya actividad principal implique tratamientos de datos que involucren una monitorización periódica y sistemática de individuos, debería nombrar necesariamente un DPO.

  Con respecto a su periodo de nombramiento, se establecía un mínimo de 2 años, pudiendo ser el DPO un empleado interno o externo, siempre que su puesto sea independencia.

- Propuesta modificación (marzo 2014): modificación criterio de obligatoriedad a:
  - realización de tratamientos que abarquen más de 5000 interesados en periodos consecutivos de 12 meses.
  - Entidades que traten "categorías especiales de datos", entendidas éstas como datos de localización, datos de menores o de empleados en grandes volúmenes, datos de salud o referentes a creencias religiosas o ideológicas.

  En lo que se refiere a la duración del periodo de nombramiento, el Parlamento Europeo respeta los 2 años establecidos por la Comisión, pero únicamente para el caso de que el DPO sea un prestador externo. Por el contrario, en el caso de que el nombramiento recayera sobren un empleado de la propia compañía, el Parlamento eleva el periodo mínimo de nombramiento a 4 años.

- Propuesta modificación (diciembre 2014): Propuesta de eliminación de la obligatoriedad del DPO, siendo voluntario.

- Se obligará a las empresas con operaciones en los estados miembros a la jurisdicción del sistema legal de los estados, incluyendo sus leyes de protección de datos. Es decir, si España opera o trata datos en Francia, deberá observar las exigencias de la ley de protección de datos francesa.

- Las compañías fuera de Europa (como Estados Unidos) seguirán estando sujetas a la legislación europea si tienen oficinas con sede en Europa o clientes europeos.

- "Privacy by design or by default", las organizaciones deberán considerar los aspectos de privacidad desde que se concibe un nuevo producto, sistema o servicio, logrando un nivel de adecuación a la norma desde el origen.

- "Privacy Impact Assessment", no existirán definidos los tres niveles de seguridad como actualmente, sino realizar análisis de riesgos en privacidad por los diferentes tratamientos de datos que se van a realizar.

- Concepto de "Accountability", referido a la responsabilidad o "rendición de cuentas", mediante el cual se pretende que las organizaciones implanten un sistema real de cumplimiento que puedan demostrar en cualquier momento en que les sea requerido

- Se prevén sanciones de entre 100 y 1.000.000 de euros o hasta un 5% de la facturación anual a nivel mundial de una empresa.

- El consentimiento expreso será la regla general. Las normas sobre consentimiento se verán fortalecidas.

- Las notificaciones de ficheros a la correspondiente Autoridad de Protección de Datos nacional quedarían eliminadas.

- Se impondrán mayores obligaciones a los Responsables de fichero y a los Encargados de tratamiento en cuanto información a los interesados sobre el tratamiento de sus datos.

- Las brechas de seguridad habrán de ser notificadas en las 24 horas siguientes a su descubrimiento a las Autoridades de Protección de Datos nacionales y a los afectados.

- Se regula el derecho al olvido.

- Se admite la posibilidad de transferir datos personales fuera de la Unión Europea sobre la base de un "equilibrio de intereses" probado.

- El Grupo del artículo 29 cambiaría su nombre al de "Consejo Europeo de Protección de Datos", y tendría un procedimiento reforzado para imponer actuaciones a las Autoridades de Protección de Datos nacionales.

- En muchos casos, la Comisión Europea se concede la facultad de emitir interpretaciones a las disposiciones del Reglamento, y no las Autoridades Nacionales como hasta ahora.

- Las asociaciones podrán presentar quejas y reclamaciones ante las Autoridades de Protección de Datos y/o acciones judiciales en nombre de las personas afectadas por una supuesta vulneración de la normativa.

En resumen, esta nueva normativa surge como respuesta de la Unión Europea a la petición de los ciudadanos europeos de otorgar un nivel más exigente de control, gestión y tratamiento de los datos. Antes de su aprobación, podrán ser comentados y modificados en un proceso legislativo de la Unión Europea que puede llevar desde varios meses a un máximo de dos o tres años.

9.7 Mala praxis en la protección de datos

En determinadas ocasiones el derecho fundamental sobre la protección de datos es utilizado no para la defensa de un principio constitucional como es el derecho al honor a la intimidad y a la propia imagen, sino que es utilizado como medida de presión con el fin de obtener beneficio en un procedimiento en el que la cuestión de fondo litigada nada tiene que ver con la solicitud de la protección de dicho derecho.

Esto puede verse reflejado en los resultados relacionados con los datos sobre los procedimientos resueltos y sancionados publicados en las Memorias de la AEPD de los años 2009 y 2010, dónde se puede comprobar el significativo incremento que han sufrido los procedimientos archivados, aumentando en un 100%.

Estos datos lo que significan es que muchos de los hechos denunciados carecen de fundamento jurídico que merezcan la apertura de un procedimiento sancionador o la imposición de una sanción económica por parte de la AEPD.

Además, la Sentencia de la Sección 1ª de la Sala de lo Contencioso de la Audiencia Nacional (SAN 1695/2011), de fecha 1 de abril de 2011, se ha pronunciado sobre esta situación al destacar que:

[*la importancia y trascendencia de la normativa sobre protección de datos y la relevancia de los derechos constitucionales que se encuentran en juego, aconsejan que no se pongan al servicio de rencillas particulares, que deben solventarse en ámbitos distintos que tengan relevancia solo en el ámbito doméstico que les es de propio, y no un ámbito como el jurisdiccional. La seriedad que conlleva el ejercicio de la potestad sancionadora aconseja que se pongan en marcha los mecanismos administrativos y jurisdiccionales correspondientes sólo cuando se suponga que se ha producido una verdadera violación del derecho fundamental a la protección de datos.*]

Con esta Sentencia, la Audiencia Nacional destaca:

- Que la normativa sobre protección de datos es lo suficientemente importante como para no utilizarse en procedimientos personales que nada tengan que ver con la razón por la cual se litiga.
- Que la mala praxis de este derecho genera unos perjuicios económicos y personales, por lo que sólo debe solicitarse cuando se haya producido una verdadera violación de los mismos.

Dentro de estos prejuicios que puede conllevar la mala praxis de este derecho se pueden encontrar los siguientes:

- Daño económico a la empresa denunciada: el derecho a la protección de datos es un derecho personalísimo que protege a las persona físicas del mal uso que se pueda hacer sobre sus datos. Por lo tanto esta normativa se dirige principalmente a sancionar a las empresas que no cumplan con los requisitos establecidos.

  Pero a diferencia de lo que ocurre en los procedimientos de derecho privado en los que el demandante puede obtener un beneficio económico y/o moral, en este tipo de procedimiento administrativo el demandante no va a obtener ningún tipo de beneficio (económico o moral), por ser la sanción impuesta una multa administrativa.

  Sin embrago, sí que puede causar un grave perjuicio económico a la empresa denunciada en caso de que la sancionen.

- Coste de medios producido por la denuncia para la Administración: tanto la AEPD, (órgano encargado del controlar el cumplimiento de la normativa sobre protección de datos), como los Tribunales de Justicia (en caso de que se recurra la resolución) van a

tener una serie de costes a la hora de archivar los procedimientos por falta de fundamentos jurídicos, que podrían traducirse en dos: económico y personal:

- En el plano económico: el coste económico se traduce en la utilización de recursos destinados a la resolución de un procedimiento, desde su apertura, o actuaciones previas, hasta el cierre de del mismo.

  La resolución de un procedimiento puede suponer determinadas como son: el desplazamiento de personal a la sede de la empresa denunciada, estudio de la documentación aportada, redacción de la resolución a emitir, etc.

- En el plano personal: en este caso el coste se produce por la pérdida de tiempo del personal destinado a un procedimiento sin base jurídica lo que puede provocar un retraso administrativo en la tramitación de los demás procedimientos.

Capítulo 10

Presupuesto

10.1 Introducción

Dentro de este capítulo se incluirá una planificación de las fases que se han llevado a cabo para el desarrollo del proyecto, junto con una valoración del presupuesto.

El proyecto ha consistido en un análisis y búsqueda de información para el entendimiento y comprensión de la normativa de protección de datos, para proceder al desarrollo de un programa de auditoría que permita obtener la relación de pruebas y aspectos a tener en cuenta de forma que sea posible valorar el grado de adecuación a la normativa o identificar las no conformidades respecto a lo establecido por la norma.

Se ha procedido a diseñar este programa de trabajo en un prototipo en Microsoft Excel que permita fácilmente su uso y distribución, así como permitir el obtener la información resultante de la valoración en Microsoft Word.

Por último se han analizado las nuevas tecnologías existentes y sus implicaciones y/o posibles riesgos respecto a la normativa de protección de datos.

10.2 Planificación

Tal y como se ha descrito en el capítulo 1, el proyecto se ha llevado a cabo en fases, a continuación presentamos la planificación de cada una de las fases y las subfases en las que se ha distribuido:

Fase/ Actividad	Fecha inicio	Duración días
Fase I: Determinación del alcance y objetivos		
Identificación objetivos y alcance	01/01/2015	7
Propuesta de contenidos	07/01/2015	15
Análisis información encuestas e importancia	12/01/2015	20
Fase II: Análisis normativa de protección de datos		
Análisis normativa europa	12/01/2015	45
Análisis normativa española	09/02/2015	60
Análisis Jurisdicción - herramientas normativas	09/03/2015	15
Análisis información Autoridades de Control	09/03/2015	10
Fase III: Análisis medidas de seguridad Título VIII		
Aspectos generales Auditoría	09/02/2015	20
MS Automatizados: análisis y definición de pruebas	09/02/2015	90
MS No Automatizados: análisis y definición de pruebas	09/02/2015	90
Fase IV: Diseño prototipo		
Análisis y definición de requisitos	09/03/2015	30
Diseño detallado	09/03/2015	90
Conexión Word y definición de Formato Informe Auditoría	15/04/2015	15
Pruebas de funcionamiento	01/05/2015	15
Depuración errores de funcionamiento	01/05/2015	15
Fase V: Evolución normativa		
Evolución normativa	15/04/2015	60
Nuevas tecnologías y nuevos retos	15/04/2015	60
Fase VI: Memoria y documentación		
Memoria y documentación	01/01/2015	160
Revisión y verificación	15/05/2015	30

Tabla 4: Planificación Fases y subfases de desarrollo

A continuación se presenta un gráfico GANTT con la planificación llevada a cabo en cada una de las fases y subfases:

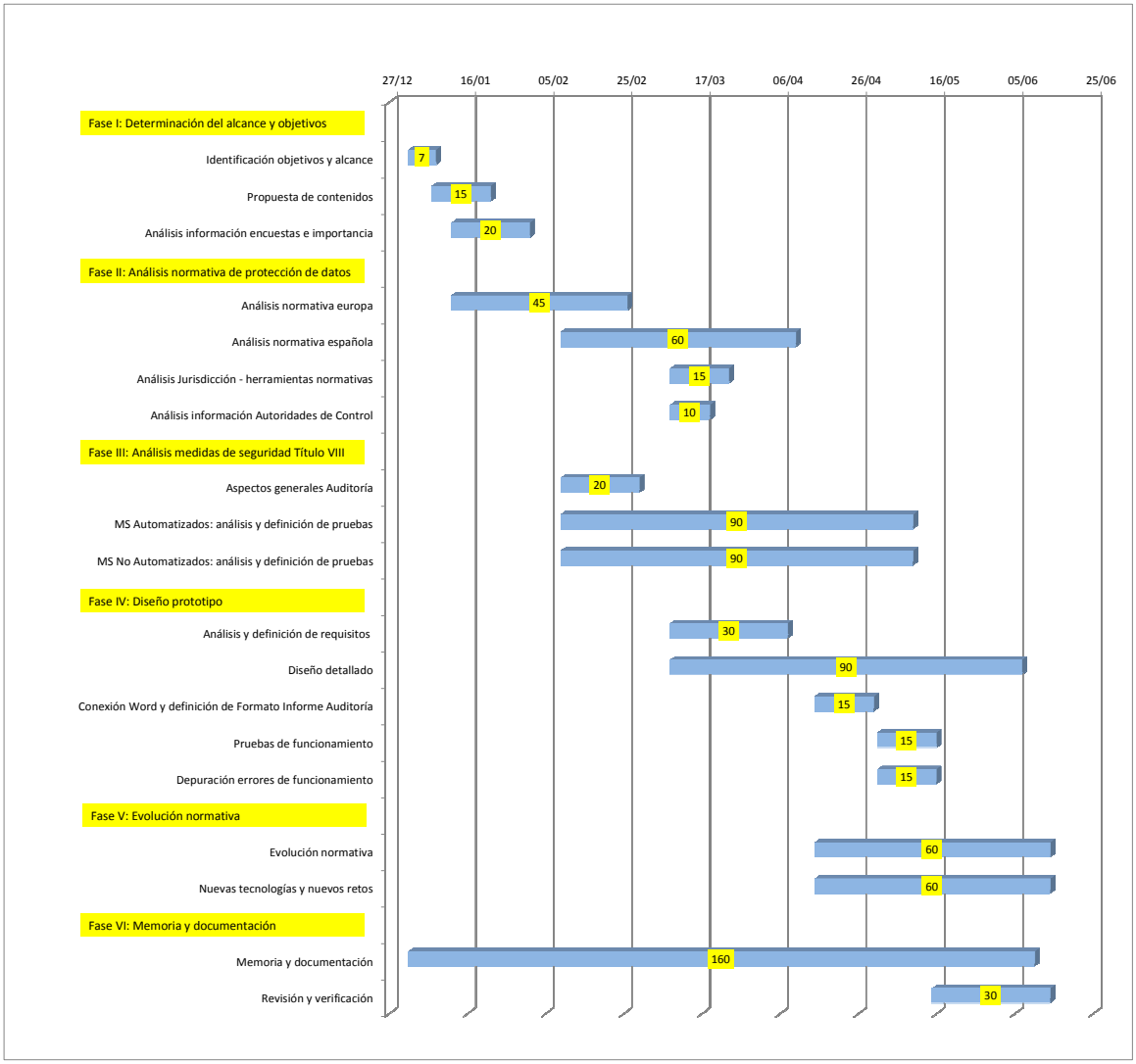


Figura 15: Gráfico GANTT Planificación

10.3 Presupuesto

A continuación se muestra el desglose de presupuesto para los recursos asignados, tiempo de dedicación y costes asociados:

UNIVERSIDAD CARLOS III DE MADRID
Escuela Politécnica Superior

PRESUPUESTO DE PROYECTO

1.- Autor: Silvia León Márquez

2.- Departamento: Informática área de Ciencias de la Computación e Inteligencia Artificial

3.- Descripción del Proyecto:

- Titulo: PROTOTIPO DE HERRAMIENTA PARA LA AUDITORÍA DE MEDIDAS DE SEGURIDAD REQUERIDAS EN LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
- Duración (meses) **5,5**
Tasa de costes Indirectos: **20%**

4.- Presupuesto total del Proyecto (valores en Euros):
Euros

5.- Desglose presupuestario (costes directos)

PERSONAL

Apellidos y nombre	N.I.F. (no rellenar - solo a título informativo)	Categoría	Dedicación (hombres mes) [a]	Coste hombre mes	Coste (Euro)	Firma de conformidad
					0,00	
Ramos González, Miguel Ángel		Ingeniero Senior	0,25	4.289,54	1.072,39	
León Márquez, Silvia		Ingeniero	5,5	2.694,39	14.819,15	
					0,00	
					0,00	
		Hombres mes	**5,75**	**Total**	15.891,53	

[a] 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)
Máximo anual para PDI de la Universidad Carlos III de Madrid de 8,8 hombres mes (1.155 horas)

EQUIPOS

Descripción	Coste (Euro)	% Uso dedicado proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable [d]
Equipo informático base: Toshiba Satellite P50-B-11M (Intel Core i7 4720HQ, Windows 8.1)	1.178,87	100	6	60	117,89
		100		60	0,00
		100		60	0,00
		100		60	0,00
		100		60	0,00
					0,00
				Total	117,89

[d] Fórmula de cálculo de la Amortización:

$$\frac{A}{B} \text{xCxD}$$

A = nº de meses desde la fecha de facturación en que el equipo es utilizado
B = periodo de depreciación (60 meses)
C = coste del equipo (sin IVA)
D = % del uso que se dedica al proyecto (habitualmente 100%)

SUBCONTRATACIÓN DE TAREAS

Descripción	Empresa	Coste imputable
	Total	0,00

OTROS COSTES DIRECTOS DEL PROYECTO[e]

Descripción	Empresa	Costes imputable
Office 2010 Proffesional	Microsoft	563,46
	Total	563,46

[e] Este capítulo de gastos incluye todos los gastos no contemplados en los conceptos anteriores, por ejemplo: fungible, viajes y dietas, otros,...

6.- Resumen de costes

Presupuesto Costes Totales	**Presupuesto Costes Totales**
Personal	15.892
Amortización	118
Subcontratación de tareas	0
Costes de funcionamiento	563
Costes Indirectos	3.315
Total	19.887

Figura 16: Presupuesto

El presupuesto total de este proyecto asciende a la cantidad de 19.887 EUROS.

Leganés a 15 de Junio de 2015

El ingeniero proyectista

Fdo. Silvia León Márquez

Capítulo 11

Conclusiones

11.1 Conclusiones principales

Por último vamos a señalar las conclusiones principales tras el desarrollo de este Proyecto Final de Carrera.

Se ha realizado una revisión de la situación actual de la normativa de protección de datos, para ello, se ha analizado tanto el marco europeo como el marco español de la protección de datos.

Este aspecto, ha sido esencial para poder determinar las medidas de seguridad tanto técnicas como organizativas que son requeridas en protección de datos y que, por tanto, los sistemas de información están obligados a cumplir.

De esta forma, es esencial que tengamos en cuenta estos aspectos en el diseño de los sistemas informáticos, para que la protección de datos se cumpla desde el diseño de los desarrollos que se llevan a cabo en una Entidad, siendo fundamental el análisis de la información desde su recogida, determinando qué tipo de información se recoge y por tanto, qué medidas de seguridad le afectan.

Se ha elaborado un programa de trabajo para llevar a cabo una revisión y/o auditoría de los sistemas de información, este programa me ha ayudado mucho para entender todas las pruebas que se deben realizar y qué aspectos hay que tener en cuenta para valorar si

los resultados de las pruebas son adecuados o si por el contrario se identifican no conformidades.

Por otro lado, se ha realizado un análisis de nuevas tecnologías y su impacto en la protección de datos, dado que la normativa tiene que cumplirse en las distintas nuevas tecnologías.

Como conclusión principal es que los principios de la protección de datos incluidos en la normativa se tienen que cumplir en las diferentes tecnologías, por lo que es necesario adaptar los distintos aspectos para que no se produzcan incumplimientos.

Glosario

AEPD	*Agencia Española de Protección de Datos*
CPD	*Centro de Procesamiento de Datos*
LOPD	*Ley Orgánica de Protección de Datos*
RLOPD	*Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos*

Referencias

Libros:

Agencia Española de Protección de datos: ‘Guía del Responsable de Ficheros’

Agencia Española de Protección de datos: ‘Guía Agencia Española de Protección de Datos Evaluación Impacto’

‘Manual del Nuevo Reglamento de Protección de Datos 2008’ (Audea Seguridad de la Información Biblioteca Empresarial Cinco Días).

‘Seguridad y Protección de datos personales’ (Ed. Thomson CIVITAS – Agencia de Protección de Datos de la Comunidad de Madrid 2009)

Dávara Rodríguez, M. A.: ‘Análisis del Real Decreto 1720/2007: El Reglamento de la LOPD’. (Ed DaFeMa 2008)

Juan Ignacio Marcos González: ‘Manual de Protección de Datos para abogados’ (Ed. Thomson Aranzadi 2008).

ECIJA Abogados: ‘Compliance. Cumplimiento normativo y seguridad en la Empresa’ (Ed. Aranzadi. Thomson Reuters 2009)

‘Cloud Computing: La Tecnología como Servicio’. Estudio publicado por el Observatorio Regional de la Sociedad de la Información de Castilla y León (ORSI)

‘Guía sobre Seguridad y privacidad de la Tecnología RFID’ (INTECO actualmente INCIBE)

‘Guía para empresas: seguridad y privacidad del Cloud Computing’ (INTECO actualmente INCIBE)

‘Guía de introducción a la Web 2.0: aspectos de seguridad y privacidad en las plataformas colaborativas’ (INTECO actualmente INCIBE)

Documentos electrónicos en la red:

Agencia Española de Protección de Datos www.agpd.org, accedido en 2014 y 2015.

‘Memoria anual AEPD’ publicada por la Agencia Española de Protección de Datos y disponible en su página web 2011.

‘Memoria anual AEPD’ publicada por la Agencia Española de Protección de Datos y disponible en su página web 2012.

‘Memoria anual AEPD’ publicada por la Agencia Española de Protección de Datos y disponible en su página web 2013 (Última publicada a la fecha de presentación de este Proyecto).

Centro de Investigaciones sociológicas - CIS www.cis.es, Estudio Número 2.812 de Septiembre de 2009, preguntas relativas a seguridad ciudadana.

Centro de Investigaciones sociológicas - CIS, Estudio Número 2.987 de Mayo de 2013, preguntas relativas a la preocupación ciudadana por la seguridad de la información y la protección de los datos personales.

Congresos o reuniones:

‘5ª Sesión anual de la AEPD’ organizada por la Agencia Española de Protección de Datos en Madrid 26 de Abril de 2013.

‘6ª Sesión anual de la AEPD’ organizada por la Agencia Española de Protección de Datos en Madrid 14 de Marzo de 2014.

‘7ª Sesión anual de la AEPD’ organizada por la Agencia Española de Protección de Datos en Madrid 21 de Abril de 2015.

‘Protección de Datos y tratamientos masivos de información’, jornada realizada por la Agencia Española de Protección de Datos con la colaboración de la Comisión Europea, en conmemoración del Día Europeo de protección de datos, 28 de Enero de 2015.