TEMA 7: LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

Gestión de Proyectos Informáticos (Bloque II)

Autores

Puntos 1-3
Juan Miguel Castillo Zaragoza
Luís Fernando Pérez Pérez
Daniel Ponsoda Montiel
Manuel Torres Mendoza

Puntos 4-6
Daniel Cano Marín
Óscar Falcó Herrera
Cristina Jiménez Femenia
Ricardo José Rodríguez Álvarez
Helena Sánchez Jiménez
Juan Sebastián Sierra Ángel

Puntos 7-9
Álvaro Gironés García
Cayetano Machón Pernis
Javier Monllor Alcaraz
Manuel Morote Herrero
Andrés Orellana Ramírez

Responsables de grupo

Juan Miguel Castillo Zaragoza
Álvaro Gironés García
Cristina Jiménez Femenia

Universidad de Alicante – Escuela Politécnica Superior
Grado en Ingeniería Informática, curso 2017/18

Tabla de contenido

1 La Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (AEPD) es un organismo con sede principal en Madrid, cuyo objetivo es velar por el cumplimento de la normativa sobre protección de datos en España.

Se trata de un ente público independiente funcionalmente, que se relaciona con el Gobierno a través del Ministerio de Justicia.

1.1 Marco normativo

La AEPD se regula por su propia normativa específica para el ejercicio de sus funciones dentro del marco de la legislación vigente. La Constitución Española de 1978, prevé en su artículo 18.4 que *"el legislador limitará el uso de la informática para proteger los derechos fundamentales de los ciudadanos"*.

Bajo esta premisa se han desarrollado a lo largo de los años varias leyes y reales decretos que han definido la Ley Orgánica de Protección de Datos (LOPD) y que conforman el estatuto y marco normativo de la AEPD.

1.2 Servicios que ofrece

Los servicios que ofrece la AEPD y que pasamos a enumerar a continuación, van dirigidos tanto a quienes tratan con los datos como a los afectados (aquellos que aparecen en los datos tratados).

1.2.1 Servicios dirigidos a los afectados

La AEPD ofrece los siguientes servicios para el ciudadano sobre quien se manejan datos:

- Informa sobre sus derechos reconocidos por ley
- Atiende sus peticiones y reclamaciones
- Promueve campañas de difusión a través de los medios
- Vela por la publicidad de los ficheros de datos de carácter personal.

1.2.2 Servicios para quienes tratan con los datos

Para toda entidad que maneja datos sensibles, (por ejemplo, entidades públicas, empresas privadas, asociaciones, etc.) la AEPD ofrece los siguientes servicios:

- Emitir las autorizaciones previstas por la Ley.
- Requerir medidas de corrección.
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
- Ejercer la potestad sancionadora en los términos previstos en el Título VII de la LOPD.
- Recabar de los responsables de los ficheros la ayuda e información que precise para el ejercicio de sus funciones.
- Autorizar las transferencias internacionales de los datos.

1.2.3 Servicios específicos en materia de telecomunicaciones

- Tutelar los derechos de los usuarios de comunicaciones electrónicas que reciben comunicaciones comerciales no solicitadas (spam).
- Recibir notificaciones de brechas de seguridad producidas en los proveedores de servicios donde el usuario esté abonado y de donde puedan filtrarse datos.

1.2.4 Otras funciones

- Elaborar e informar de normas, instrucciones y recomendaciones en materia de LOPD.
- Cooperación con organismos internacionales

1.3 Resoluciones más controvertidas

A continuación, describimos a modo de ejemplo algunas de las resoluciones de la AEPD que han causado más polémica a lo largo de su historia como resultado de su más rigurosa aplicación de la LOPD:

- En 2008, el Tribunal Supremo declara que los libros de bautismo de la Iglesia no son ficheros de datos, y por tanto desautoriza a la AEPD, quien había dado la razón a un solicitante de cancelación.
- Las opciones de "enviar a un amigo" o de "recomendar página" de ciertas webs, también han sido sancionadas en aplicación de la LOPD.
- Se ha sancionado a aseguradoras y centros de salud que intercambian información médica sobre los pacientes sin consentimiento expreso. Sin embargo, dicha sanción ha sido reducida por no haber mostrado intencionalidad de infracción.
- La AEPD sancionó a una empresa que, tras sufrir el ataque de un hacker, se vio chantajeada por éste quien posteriormente la denunció por el agujero de seguridad que encontró.
- En 2018 la AEPD sanciona a WhatsApp y Facebook por usar datos personales sin consentimiento.

2 Registro de ficheros

2.1 ¿Qué son?

"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" *(Artículo 3.b de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y artículo 5.1.k del Real Decreto 1720/2007).*

En base a esta definición, podemos determinar que un fichero es un conjunto de datos personales organizados, que pueden ir desde nombre, apellidos, DNI/NIF hasta orientación sexual o ideológica. Es importante destacar que, independientemente de que el acceso a los datos se lleve a cabo de forma manual (p. ej. papel) o a través de procedimientos informáticos (p. ej. bases de datos) siempre se tratará con ficheros en el ámbito legal.

2.2 Tipos de ficheros.

En base a esto, la normativa distingue entre ficheros no automatizados y automatizados, centrándonos nosotros en estos últimos.

- Ficheros automatizados: Ficheros que se almacenan la información en soportes informáticos (bases de datos, archivos, carpetas etc.).

Se dividirá el tipo del fichero según el ámbito de la organización que tenga la posesión de estos, pudiendo ser público o privado.

- Ficheros de titularidad pública: Su titular es una entidad pública (Administración pública, gobierno...etc.). Además, el uso de estos datos debe de estar dirigido al desarrollo de una actividad pública. Por ejemplo:
    - Rentas económicas sobre las familias que solicitan una beca al ministerio de educación.

  - Antecedentes policiales e información personal de personas que se usan en el sistema judicial.
- Ficheros de titularidad privada: Su titular puede ser tanto un particular como una empresa o incluso una entidad pública, siempre y cuando los datos vayan dirigidos a una actividad no pública.
  - Datos personales (bancarios, localización, descriptivos…) de Amazon sobre un cierto usuario, usados para poder ejercer su actividad de venta de productos, tanto envío como pagos.
  - Información que suben los usuarios al sistema de almacenamiento 'Dropbox'.

2.3 Inscripción en el Registro de la Agencia Española de Protección de Datos. ¿Por qué debemos registrar los ficheros?

Podemos decir que hay dos motivos fundamentales para estar a favor y utilizar el registro de ficheros en la Agencia de Protección de Datos Española:

1. Por qué la ley nos obliga, ya que lo cierto es que el artículo 26 de la Ley de Protección de Datos de 1999 nos obliga a inscribir los ficheros que tengamos que contengan datos personales. De esta forma el gobierno obliga a justificar la utilización de ciertos datos en nuestra aplicación, debido, ni más ni menos, a que todo español tiene el derecho a la intimidad y por consiguiente, a la privacidad de su información personal según el artículo 18 de la constitución española.
2. Sabemos que el mundo funciona en base a un marco económico global, el cual influye de forma inmediata sobre este, todo ello para perseguir el objetivo de un mayor desarrollo financiero. Hoy en día, los datos de carácter personal pueden ser utilizados en mecanismos ilegales para conseguir el objetivo nombrado anteriormente.

De este segundo apartado, podemos nombrar algunos ejemplos derivados del comercio en la "Internet profunda" con datos personales, en muchas ocasiones vendidas por las mismas compañías que los almacenaban. Por supuesto, a espaldas de la AEPD, ya que no se reflejaba en el apartado de "Transferencias a países terceros" del que luego hablaremos.

2.4 ¿Cómo realizar la inscripción?

Aunque se puede llevar a cabo de forma presencial, la opción más popular es la que utiliza el servicio electrónico NOTA, el cual permita la inscripción a través de Internet (con y sin certificado de firma electrónica reconocido).

Algo que debemos de tener en cuenta es que el registro, o el alta, de un nuevo fichero se debe efectuar antes de la realización de este. Es decir, si sabemos que vamos a tener una base de datos para nuestro sitio web, ANTES de crear la base de datos debemos de dar de alta el fichero con los datos que vamos a tener. De igual forma, si prevemos que vamos a tener 4 bases de datos, deberemos de dar de alta 4 ficheros previamente. Por el contrario, si se va a modificar un fichero existente o a eliminar, se debe de informar a la Agencia Española de Protección de Datos de igual forma, eso sí, no hará falta crear un nuevo fichero, pudiendo hacer referencia al creado anteriormente.

Podemos realizar el registro del fichero en la siguiente URL: https://sedeagpd.gob.es/sede-electronica-web/vistas/formNOTA/servicioNOTA.jsf. Los datos necesarios se enumeran a continuación.

2.4.1 Ámbito de la organización

En primer lugar, nos preguntará por el ámbito de la organización que quiere llevar a cabo el registro (pública o privada), además de elegir la opción con o sin certificado de firma electrónica. Obviamente, si se hace sin certificado se deberá de imprimir, firmar y presentar el documento generado a la AEPD.

2.4.2 Datos personales del declarante

Se preguntará por los datos personales del declarante. Cabe destacar que el declarante tiene que ser la misma persona que el responsable del fichero si estamos representando a una persona física (autónomo), en el caso de una empresa, debemos de introducir el nombre de la empresa como responsable del fichero.

Cargo: Si el responsable del fichero vas a ser tu mismo entonces puedes poner “Responsable del fichero”, si el responsable va a ser una empresa por ejemplo puede poner “Administrador”

Medio de notificación: Existen dos opciones “Correo Postal” y “Sede electrónica”, la primera opción recibiremos una carta (Puede tardar un mes o más), en cambio en sede electrónica recibiremos un correo cuando la notificación haya sido resuelta (unos 4 días).

2.4.3 Datos personales del responsable del fichero.

El responsable del fichero es el que debe cumplir con todas y cada una de las obligaciones de la LOPD, y el que responderá ante cualquier infracción de esta, además de decidir sobre la finalidad, uso y contenido de este.

2.4.4 Datos personales del responsable de los derechos de ARCO.

En primer lugar, los derechos de ARCO son un conjunto de derechos que se le ofrecen al ciudadano sobre el Acceso, Rectificación, Cancelación y Oposición de los datos registrados en el fichero.

- Derecho de acceso: El ciudadano puede ponerse en contacto con el responsable del fichero para preguntar el origen de los datos, y la finalidad del tratamiento de estos para su organización.
- Derecho de rectificación y cancelación: El ciudadano puede imponer al responsable del fichero que rectifique (modifique) los sus datos o bien que los cancele (elimine), siempre y cuando los datos del ciudadano sean inexactos, incompletos, inadecuados o excesivos.
- Derecho de oposición: El ciudadano puede dirigirse al responsable del fichero para que se dejen de tratar sus datos si estos se están utilizando sin su consentimiento o cuando sus datos se están usando en fines publicitarios o de prospección comercial.

En este apartado proporcionamos los datos de la oficina donde el ciudadano puede consultar cualquier tema relacionado con sus derechos de arco.

2.4.5 Información personal sobre el encargado del tratamiento.

Si una entidad externa (empresa de contabilidad, marketing…) va a tratar datos personales de algún fichero se debe de asociar información personal del responsable de esta entidad.

2.4.6 Identificación y finalidad del fichero.

En el apartado de "Denominación", debemos definir un nombre para identificar el fichero, además de especificar una descripción de la finalidad y usos previstos de los datos personales. Estos apartados son muy importantes, ya que debemos de justificar por qué almacenamos estos datos personales y que actividad desarrollan.

Por último, el apartado de "Tipificación" es una lista de finalidades de la cual tenemos que elegir aquella que mejor se adapte a nuestro fichero.

Ejemplo: Empresa comercial. Todos los ficheros destinados a gestionar las operaciones comerciales que se llevan a cabo con los clientes formarían un único fichero con título "Gestión de clientes", con una descripción "fichero para la gestión integral de las relaciones comerciales con los clientes" y una finalidad "Gestión de clientes, contable, fiscal y administrativa".

2.4.7 Origen y procedencia de los datos.

Origen de los datos y colectivos de los que proceden los datos. EJEMPLO: Para una tienda online, podríamos seleccionar en "Origen" la opción "El propio interesado o su representante legal" y para "Colectivos o categorías de interesados" las opciones "CLIENTES Y USUARIOS" y "PROVEEDORES".

2.4.8 Tipos de datos, estructura y organización.

Se especifica qué tipo de datos contiene el fichero, religiosos, identificativos, etc. Este es un apartado importante, ya que guardar uno u otro tipo de datos implicará tener un nivel de seguridad determinado.

(NOTA: Sistema de tratamiento en nuestro caso, casi siempre será automatizado).

2.4.9 Cesión o comunicación de datos.

En este apartado se debe de informar a la AEPD si se van a transferir datos a otra organización para cumplir un fin determinado que beneficie a la organización que proporciona los datos, p. ej. contabilidad, fiscalidad...etc.

(NOTA: Cuando se le da el control de los datos a un tercero para la contabilidad u otro asunto, por ejemplo, el caso visto anteriormente del responsable del servicio no es una transferencia de datos.)

2.4.10 Transferencias internacionales.

Si vamos a transferir datos a un país que no pertenezca al marco europeo, debemos de comunicarlo en este apartado. Esta es una opción muy utilizada por organizaciones que no tienen sus servidores en Europa y necesitan transferir datos a estos.

3 El documento de seguridad

El *documento de seguridad* es el documento mediante el cual se elabora y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal. Su adopción es de obligado cumplimiento para el encargado del fichero, o en su caso, el encargado del tratamiento.

Aunque es ampliable bajo el criterio de la persona encargada de la seguridad de la información del sistema está formado básicamente por estos cinco puntos:

3.1 Ámbito y aplicación del documento

En este apartado se detallará el nombre de la persona responsable de la seguridad de los ficheros, así como un listado con todos los documentos o procedimientos inherentes a estos indicando si se trata de un sistema automático, manual o mixto y que nivel de seguridad le corresponde.

Por cada apartado del listado se adjuntará un anexo en el que se realice una descripción detallada de cada uno de los ficheros y los aspectos que le afecten de forma particular.

3.2 Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos en este documento.

En este apartado se describirá detalladamente toda la información necesaria sobre los siguientes puntos contando con *plantillas básicas para rellenar los huecos necesarios en la web de la LOPD:*

a) Medidas de identificación y autenticación de los usuarios en el sistema
b) Controles de acceso al sistema
c) Registro de accesos al sistema
d) Gestión de soportes y documentos existentes en el sistema
   - Registro de entrada y salida de soportes
   - Gestión y distribución de soportes
   - Criterios de archivo
   - Almacenamiento de la información
   - Custodia de soportes
e) Acceso a datos del sistema a través de redes de comunicaciones
f) Régimen de trabajo fuera de los locales de la ubicación del fichero
g) Normas de traslado de documentación
h) Ficheros temporales o copias de trabajo de documentos
i) Copia o reproducción de los mismos
j) Procedimiento para copias de respaldo y recuperación
k) Persona/s responsable/s de seguridad de las medidas reflejadas en este sistema

3.3 Información y obligaciones del personal

En este apartado se describirá detalladamente toda la información necesaria sobre los siguientes puntos:

a) Procedimiento de información al personal sobre la gestión de los datos.
b) Funciones y obligaciones del personal en relación con estos.
c) Consecuencias del incumplimiento del documento de seguridad.

3.4 Procedimientos de notificación, gestión y respuesta ante las incidencias

En este apartado del documento se detallará paso a paso el procedimiento de notificación, gestión y respuesta ante las incidencias que puedan acontecerse durante el tratamiento de los datos del sistema, persona a informar, modo de hacerlo, medidas a llevar a cabo, etc.

3.5 Procedimientos de revisión

Procedimiento de revisión del documento de seguridad con el fin de que se siga adaptando a la normativa en el caso de haberse producido cambios en el sistema de información de la empresa.

4 El personal involucrado.

4.1 Encargado del tratamiento. Derecho y obligaciones.

Se entenderá por encargado del tratamiento: La persona física o jurídica, servicio o cualquier otro organismo que, solo o con otros, trate datos personales por cuenta del responsable del tratamiento.

El encargado de tratamiento 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 tampoco los comunicará. En caso de incumplir el contrato, será también considerado el responsable de tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Infracciones:

- Leves. De 60€ a 60.100€ de multa.
- Graves. De 60.100€ a 300.500€ de multa.
- Muy graves. De 300.500€ a 601.000€ de multa.

4.2 Responsable de seguridad

El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas de seguridad del documento.

Este revisará al menos una vez al mes la información de control registrada y elaborará un informe. Una vez realizado, se encargará de elevar sus conclusiones al responsable del fichero para que adopte las medidas adecuadas.

4.3 Delegación de autorizaciones

Personas en las que el responsable del fichero ha delegado, tales como: salida de dispositivos portátiles, la copia o reproducción de documentos en soporte digital, papel, etc.

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.

4.4 Descripción del sistema informático y perfiles de usuarios.

Todas las personas físicas, empresas o instituciones que mantengan ficheros con algún tipo de información de carácter personal, y que además afectan a sistemas informáticos, se consideran responsables de un fichero y, por tanto, deberán adoptar las medidas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En cuanto a los perfiles, si un usuario particular crea un perfil en cualquier sistema informático, puede llegar a estar excluido del cumplimiento de la normativa de protección de datos. Sin embargo, cuando es una empresa la que se registra y obtiene información de sus contactos (pudiendo llegar a ser, de carácter personal) lo hace con ánimo de lucro, en este caso, sí está obligada al cumplimiento de la LOPD.

4.5 Procedimiento general de información al personal. Funciones y obligaciones del personal.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con un procedimiento establecido.

4.5.1 Funciones y obligaciones del personal

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Constituye una obligación del personal notificar las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos.

4.6 Procedimiento para la recogida de datos

Los responsables de ficheros o tratamientos (empresas, Administraciones Públicas u otras entidades) a los que has facilitado tus datos de carácter personal deben cumplir con unos principios y obligaciones que se regulan en la conocida como LOPD (Ley Orgánica 15/1999, de 13 de diciembre) y el Reglamento que la desarrolla (Real Decreto 1720/2007, de 21 de diciembre).

Uno de estos principios es el de Calidad que supone que cuando se recaben tus datos de carácter personal deben cumplirse las siguientes premisas:

- Solo podrán utilizarse para una finalidad determinada.
- No podrán recabarse datos que sean excesivos.
- Su recogida debe ser proporcional a la finalidad para la cual se van a utilizar los datos.
- No pueden utilizarse para una finalidad incompatible de la que motivó su recogida y tratamiento.

Prosiguiendo, como dice el artículo 5 “Derecho de información en la recogida de datos” de la LOPD, se tiene que informar a la persona afectada de los siguientes apartados:

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.

Para finalizar se deben de cumplir los siguientes apartados en lo referente al consentimiento según lo dispuesto en el artículo 6 de la LOPD:

a) El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
b) 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
c) El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
d) 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 de fichero excluirá del tratamiento los datos relativos al afectado.

4.7 Derecho de acceso

A través del ejercicio de este derecho la persona afectada puede conocer qué datos de carácter personal están siendo tratados por parte del responsable, la finalidad de este tratamiento, el origen de los citados datos y si se han comunicado o se van comunicar a un tercero. Una vez que haya ejercitado su derecho de acceso, deben de contestarle en el plazo máximo de un mes, y en caso de estimar su derecho, el acceso se hará efectivo en el plazo máximo de diez días hábiles, pudiendo elegir la forma por la cual va a recibir la información a través de alguno de los siguientes medios:

- Visualización en pantalla.
- Escrito, copia o fotocopia remitida por correo, certificado o no.
- Telecopia.
- Correo electrónico u otros sistemas de comunicación electrónica.
- Cualquier otro sistema adecuado ofrecido por quien posee sus datos personales (responsable del fichero).

4.8 Derecho rectificación y cancelación

El derecho de rectificación permite que modifique aquellos datos que sean inexactos o incompletos, indicando en la solicitud de rectificación qué datos desea que se modifiquen. A esta solicitud deberá acompañar la documentación justificativa correspondiente.

Por otra parte, el derecho de cancelación permite la cancelación de tus datos personales que sean inadecuados o excesivos. No obstante, se conservarán bloqueados de manera que se impida su tratamiento, sin perjuicio de su puesta a disposición de las administraciones públicas, jueces y tribunales, para la atención de las posibles responsabilidades que hayan surgido del tratamiento durante su plazo de prescripción. Cumplido este plazo se procederá a la supresión de los mismos.

Cuando solicite la cancelación de sus datos personales, deberá indicar a qué datos se refiere, aportando la documentación que justifique tal pretensión. Le deben contestar en el plazo máximo de 10 días hábiles. Si sus datos hubieran sido comunicados a un tercero, el responsable deberá comunicarle los datos cancelados para que, a su vez, este tercero los cancele.

4.9 Derecho de oposición

Mediante el ejercicio de este derecho puedes oponerte a que no se realice el tratamiento de tus datos personales en los siguientes supuestos:

- Cuando no siendo necesario tu consentimiento para el tratamiento de tus datos, exista un motivo legítimo y fundado referente a tu concreta situación personal (salvo que una Ley establezca lo contrario).
- Cuando no siendo necesario tu consentimiento para el tratamiento de tus datos, exista un motivo legítimo y fundado referente a tu concreta situación personal (salvo que una Ley establezca lo contrario).
- Cuando el tratamiento tenga como fin la adopción de una decisión referida a ti basada únicamente en un tratamiento automatizado de tus datos personales.

Cuando se ejercita este derecho, al igual que en el de rectificación, deben contestar en el plazo máximo de 10 días hábiles.

4.10 Procedimientos de ejercicio de los derechos de los afectados

El titular de los datos de carácter personal puede ejercitar ante el responsable del fichero que esté tratando o gestionando sus datos los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) siendo todos independientes entre sí.

El procedimiento para ejercer estos derechos es el siguiente:

1. Petición dirigida al responsable que posea sus datos personales.
2. Fotocopia del DNI o pasaporte u otro documento válido que le identifique.
3. Si los ejercitas a través de un representante, documento o instrumento electrónico que acredite la representación.
4. Petición en que se concreta la solicitud.
5. Dirección a efectos de notificaciones, fecha y firma.
6. Documentos acreditativos de la petición que realice, si fuesen necesarios.

5 Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar los niveles de seguridad exigidos.

Se definen tres niveles de seguridad aplicables a los ficheros que pasamos a detallar a continuación:

El nivel básico se aplica a todos los ficheros, mientras que el nivel medio se aplica a los siguientes:

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.

El nivel alto se aplica a los datos de ideología, afiliación sindical, origen racial, salud, vida sexual, datos para fines policiales o delitos.

Algunas medidas de seguridad que se deben de realizar en función del nivel de seguridad que declaremos tener están recogidas en esta tabla resumen:

Medidas de seguridad	Nivel Basico	Nivel Medio	Nivel Alto
Art 89. Funciones y obligaciones del personal	Si	Si	Si
Art 90. Registro de incidencias	Si	Si	Si
Art 91. Control de acceso	Si	Si	Si
Art 92. Gestión de soportes y documentos	Si	Si	Si
Art 93. Identificación y autenticación	Si	Si	Si
Art 94. Copias de respaldo y recuperación	Si	Si	Si
Art 95. Responsable de seguridad	------	Si	Si
Art 96. Auditoria	------	Si	Si
Art 97. Gestión de soportes y documentos	------	Si	Si
Art 98. Identificación y autenticación	------	Si	Si
Art 99. Control de acceso físico	------	Si	Si
Art 100. Registro de incidencias	------	Si	Si
Art 101. Gestión y distribución de soportes	------	------	Si
Art 102. Copias de respaldo y recuperación	------	------	Si
Art 103. Registro de accesos	------	------	Si
Art 104. Telecomunicaciones	------	------	Si

5.1 Identificación y autenticación

Medidas y normas relativas a la identificación y autenticación del personal autorizado para acceder a los datos personales:

- Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales, de forma inequívoca y personalizada. Cada identificación debe pertenecer a un único usuario.
- Si la autenticación se realiza mediante contraseña, detallar el procedimiento de asignación, distribución y almacenamiento de la misma, así de la periodicidad con la que se deberá cambiar. (Incluir, además, los requisitos que deben cumplir las cadenas utilizadas como contraseña).
- Nivel medio: en los ficheros de nivel medio y alto, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.

5.2 Ficheros temporales o copias de trabajo de documentos

Son creados exclusivamente para trabajos temporales deben cumplir las medidas de seguridad descritas en el Reglamentos y serán borrados una vez dejen de ser necesarios.

Para los ficheros de alto nivel, las copias de los documentos con datos personales sólo se pueden llevar a cabo bajo el control de personal autorizado: Indicar los usuarios autorizados.

Las copias desechadas deberán ser destruidas asegurando el posterior acceso a la información. Se debe indicar al usuario las diferentes maneras en las que puede realizar esa destrucción.

5.3 Otras medidas

A continuación, se enumeran una serie de medidas que se deben de adoptar también para garantizar los niveles de seguridad exigidos. Estos puntos se explicarán con más detalle en los siguientes apartados del tema:

- Control de acceso
- Régimen a seguir para datos desubicados de los locales
- Copias de respaldo y recuperación

6 Control de accesos.

6.1 Locales y equipamientos.

Los locales donde se ubiquen los sistemas de información que contienen los ficheros con datos de carácter personal deben de ser objeto de especial protección de forma que garanticen la disponibilidad, confidencialidad e integridad de los datos protegidos. Dichos locales deberán contar con las medidas mínimas de seguridad que eviten accesos no autorizados ya que el acceso estará restringido exclusivamente al personal autorizado.

Dependiendo del nivel de seguridad del fichero a albergar, se estipulan diferentes controles de acceso: básico, medio y alto.

Todo local que albergue en su interior algún documento de nivel medio o superior deberá tener control de acceso físico al local en el cual se alberguen dichos documentos, incluyendo con esto a los equipamientos del interior del local.

6.2 Control de acceso físico

- El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. El responsable del fichero establecerá mecanismos para evitar que el usuario pueda acceder a recursos con derechos distintos de los autorizados.
- Exclusivamente la persona autorizada puede conceder, alterar o anular el acceso sobre los datos y recursos, conforme a los criterios establecidos por el responsable del fichero.
- De existir personal ajeno responsable del fichero con acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

6.3 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 deberán hacerse constar expresamente en el documento de seguridad.

6.4 Ficheros automáticos

Tal y como establece el artículo 91 del Real Decreto 1720/2007, en todos los ficheros automatizados se debe implantar un mecanismo que controle el acceso de los usuarios a los datos de carácter personal en los siguientes términos:

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.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

6.5 Ficheros manuales

En el caso de los ficheros manuales con nivel alto de seguridad, el Reglamento de la LOPD establece, en su artículo 113 las medidas que han de adoptarse para controlar el acceso a la documentación a la que deba implantarse las medidas de nivel alto.

Para implantar este control de acceso a la documentación se podrán utilizar, por ejemplo:

- Plantillas básicas en soporte papel incorporadas al inicio del expediente.
- Registros automatizados en la gestión de entradas y salidas al archivo.
- Cualquier otro sistema o procedimiento que permita alcanzar la finalidad perseguida por el reglamento.

7 Gestión y soporte de documentos

Como soportes entenderemos todo objeto físico que almacena o contiene datos de carácter personal tanto automatizados (Disco duro Externo, USB, CD, etc.) como no automatizados (Archivadores AZ, Carpetas, y demás dispositivos que guarden datos de carácter personal) y que sean susceptibles de ser tratados en un sistema de información. El inventario de soportes es una de las medidas de seguridad de la LOPD sobre la que menos cuidado se pone por parte de los usuarios de los ficheros.

Cada año, la Agencia Española de Protección de Datos sanciona a las empresas por encontrar soportes (principalmente, disquetes, discos duros y papel) que aparecen en lugares donde no deberían encontrarse, incumpliendo una de las medidas de seguridad básicas de la LOPD como es el inventario de soportes. Para que no nos sancionen debemos de realizar los siguientes pasos:

1. Los soportes y documentos deberán de identificar su contenido, ser inventariados y solo podrán ser accedidos por el personal autorizado en el documento de seguridad. En el caso de no poder garantizar estas medidas, se deberá dejar constancia en el documento de seguridad.
2. El traslado de los soportes y documentos deberá realizarlo el personal autorizado en el documento de seguridad. Siempre que se proceda a un traslado físico de la documentación se deberán adoptar medidas para impedir el acceso o manipulación a dichos documentos.
3. Durante el traslado se tomarán medidas dirigidas adaptadas a evitar la sustracción, pérdida o acceso indebido.
4. Los soportes y documentos desechados deberán de ser borrados o destruidos de forma que se evite el acceso a los datos o su posible recuperación.
5. Los soportes con información sensible podrán ser etiquetados de distinta forma, con tal de que el personal autorizado pueda identificar su contenido y que dificulte el reconocimiento del personal no autorizado.

Para más información acerca de esta información, consultar el Art.92 del BOE.

7.1 Criterios de archivo. Art.106

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deben garantizar la correcta conservación de los

documentos, la localización, consulta de la información y derecho a no tratar los datos salvo que lo autorice una norma con rango de ley (mirar Art.10) , 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.

7.2 Almacenamiento de ficheros manuales. Art.107 y Art.111

Los dispositivos deben disponer de mecanismos que obstaculicen su apertura. De no disponerlos, el responsable del fichero deberá adoptar las medidas que impidan el acceso al personal no autorizado.

Los ficheros no automatizados, deben encontrarse en áreas con puertas de acceso bajo llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas mientras no se consulten. En su defecto, el responsable deberá tomar medidas alternativas que se incluirán en el documento de seguridad.

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.

7.3 Custodia de soportes manuales Art.108 y Art.109

Mientras los datos no se encuentren archivados, la persona a cargo de los documentos deberá impedir el acceso de toda persona no autorizada. Se designarán uno o varios responsables cuyas funciones se contemplan en el Art.95

7.4 Seguridad en la reutilización o eliminación soportes y documentos. Art. 112

Sobre la reutilización de soportes y documentos, sólo el personal autorizado en el documento de seguridad podrá realizar la reproducción de los documentos.

En cuanto a la destrucción, lo más recomendable para informes en papel o '*CDs*' que contengan datos de carácter personal más sensible y no sean voluminosos, es destruirlos en una destructora de papel, o si tienes datos especialmente protegidos o sensibles, contratar a una empresa destructora homologada que certifique la destrucción. Todo esto de una forma segura y confidencial, que haga constar los procedimientos o mecanismos adoptados y el momento en que se efectuó la destrucción definitiva.

En caso de no existir máquina destructora de papel y '*CDs*' o en el caso de que los listados e informes sean muy voluminosos, deberán ser depositados en unos contenedores confidenciales herméticos para ser entregados a una compañía de reciclaje que garantice mediante contrato la destrucción de los mismos.

El objetivo final de la destrucción es que ya no se pueda acceder a la información contenida o recuperar la copia que hemos destruido. Como hemos comentado en el artículo 92.4.

7.5 Registro de entradas y salidas de soportes Art.113

- Acceso limitado a personal autorizado.
- Habilitar mecanismos de identificación de acceso para documentos con acceso de múltiples usuarios.
- El acceso de personas no incluidas en el anterior párrafo deberá quedar registrado.

7.6 Acceso a datos a través de redes de comunicaciones Art.85y Art.104

Las redes deben garantizar un nivel de seguridad equivalente al acceso en modo local. La transmisión debe ser cifrada o con otro mecanismo que garantice que la información no sea legible ni manipulada por terceros.

8 Copias de seguridad

Para asociar las copias de seguridad dentro de la LOPD, previamente debemos de tener claro el concepto "Copia de seguridad".

¿Qué es una copia de seguridad?

"*Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.*"

El proceso de copia de seguridad se complementa con el de restauración de los datos, que consiste en recuperar los datos de la copia de seguridad, ya sea en la ubicación original o en otra ubicación elegida.

¿Por qué son importantes las copias de seguridad?

- Las copias de seguridad son útiles ante distintos eventos:
- Recuperar los sistemas informáticos de un ataque cibernético.
- Restaurar datos que pueden haberse eliminado accidentalmente.
- Restaurar datos corrompidos.
- Restaurar datos infectados por un virus informático.
- Prevenir ante posibles robos, pérdidas o roturas de los dispositivos donde almacenas tus datos.

8.1 Técnicas de copia de seguridad

Es fundamental un mecanismo de copia de seguridad que asegure la continuidad y recuperación de todos los datos importantes de una compañía, sin interrumpir el funcionamiento del sistema informático. Es importante elegir el mecanismo adecuado atendiendo a las necesidades de nuestro sistema, indicando de qué datos se hará copia, con qué frecuencia, con qué método y como recuperar esos datos si hiciera falta

Por lo general, las copias de seguridad se dividen en las siguientes categorías:

- Copia de seguridad completa
    - La copia de seguridad completa realiza una copia fiel de los datos en un medio aparte.
    - Ventajas:
        - Proporciona una imagen fiable de los datos a través del tiempo.
    - Inconvenientes:
        - Lenta en grandes volúmenes de datos, si estos se están modificando durante dicho proceso.
        - Puede causar problemas de disponibilidad en grandes volúmenes de datos ya que crea discos de acceso pesado, grande y costoso.
- Copia de seguridad incremental

    - La copia de seguridad incremental consiste en copiar todos los elementos que han sido modificados desde la copia de seguridad anterior de cualquier tipo.
    - Ventajas:
        - Más eficaz que una copia de seguridad completa, ya que se centra específicamente en los archivos modificados y requiere menos espacio de almacenamiento.
    - Inconvenientes:
        - Es necesario contar con las copias de seguridad anteriores para restaurar la copia de seguridad completa.
- Copia de seguridad diferencial
    - La copia de seguridad diferencial se centra específicamente en los archivos que han sido modificados desde la última copia de seguridad completa, por lo que seguramente almacenará más datos que una copia de seguridad incremental, pero menos que una completa.
    - Ventajas:
        - Más fiable que la copia de seguridad incremental.
    - Inconvenientes:
        - Más lenta y costosa en cuanto a espacio de almacenamiento que la copia de seguridad incremental.

8.2 Políticas de copia de seguridad

- Diferenciar entre distintos entornos (preproducción, desarrollo, test, producción, etc.)
- Determinar los costes de las posibles pérdidas de datos
- El tiempo que se tardaría en la recuperación
- Valorar los recursos disponibles (hardware, velocidad de la red, discos remotos, etc.)
- Analizar qué es imprescindible copiar y qué no.

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la Política de seguridad en lo relativo a copias de seguridad. Los controles se clasifican en dos niveles de complejidad:

- Requerimientos básicos:
    - La copia debe ser con periodicidad semanal, a menos que no haya modificación de los datos. (en la práctica suele ser diaria)
    - El proceso de copias debe garantizar que los datos se recuperarán al momento previo a cualquier incidente.
    - Cada 6 meses debe comprobarse el correcto uso del sistema de copias de seguridad.
    - En caso de realizar pruebas para la implantación o modificaciones de los sistemas de seguridad, previamente deberá realizarse una copia de seguridad.
- Alto:
    - más de todo lo contemplado en el nivel básico, debe conservarse una copia de respaldo en “un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan”.

8.3 Procedimientos verificación y recuperación.

8.3.1 Verificación

Muchos programas de copia de seguridad hacen uso de Sumas de verificación o '*hashes*'. Esto ofrece muchas ventajas. Primero, estos permiten a la integridad de los datos ser verificados sin

hacer referencia al archivo original: si el archivo guardado en un medio de copia tiene la misma suma de verificación que el valor salvado, después es muy probable que sea correcto. Segundo, algunos programas de copias de seguridad pueden usar sumas de verificación para evitar hacer redundantes copias de archivos, y así mejorar la velocidad de la copia de seguridad. Esto es particularmente útil en procesos de reduplicado.

Recuperación simple:
El modelo de recuperación simple proporciona la forma más sencilla de realizar copias de seguridad y restauración. Este modelo de recuperación admite copias de seguridad de bases de datos y de archivos, pero no admite copias de seguridad de registros. Solo se hace copia de seguridad de los datos del registro de transacciones con los datos del usuario asociado. La ausencia de copias de seguridad de registros simplifica la administración de realización de copias de seguridad y restauración. . Sin embargo, una base de datos solo se puede restaurar al final de la copia de seguridad más reciente.

Recuperación completa:
En el modelo de recuperación completa se usan copias de seguridad de registros para evitar la pérdida de datos en la mayor parte de los casos de error, siendo necesario realizar copias de seguridad y restaurar el registro de transacciones (copias de seguridad de registros). La ventaja de usar las copias de seguridad de registros reside en que permite restaurar una base de datos a cualquier momento de una copia de seguridad de registros (recuperación a un momento dado). Puede utilizar una serie de copias de seguridad de registros para poner al día una base de datos hasta cualquier momento que se encuentre en una de las copias de seguridad de registros. Tenga en cuenta que para reducir el tiempo de restauración, puede complementar cada copia de seguridad completa con una serie de copias de seguridad diferenciales de los mismos datos.

8.3.2 Restauración

El objetivo final de un '*backup*' es poder restaurarlo en caso de pérdida de los datos. Por lo tanto, tener presente la restauración a la hora de definir una política de '*backups*' o escoger una herramienta es clave. Para ello, es importante haber decidido previamente (en la gestión de riesgos) los siguientes puntos:

- RTO (Recovery Time Objective)
    - Es el tiempo máximo en el que se debe alcanzar un nivel de servicio mínimo tras una caída del servicio (por ejemplo, debido a pérdida de datos) para no causar consecuencias inaceptables en el negocio.
- RPO (Recovery Point Objective)
    - Es el periodo de tiempo máximo en el que se pueden perder datos de un servicio. Si el periodo de tiempo es de 6 horas, se deben realizar '*backups*' cada menos tiempo y poder recuperar la información antes de agotar el periodo.

El tiempo de restauración de un '*backup*' en caso de pérdida de datos forma parte del tiempo en que no hay servicio, por lo que cuanto menos tarde antes se restablecerá el proceso de negocio.

9 Seguimiento y control (Auditoría LOPD).

La finalidad de la auditoría y su informe es identificar las no conformidades existentes, la adecuación de las medidas y controles a la Ley de Protección de Datos, su desarrollo reglamentario y propone las medidas correctoras o complementarias necesarias para el debido cumplimiento legal. Incluye, además, los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

9.1 Controles periódicos

En las empresas con un nivel de seguridad medio o superior. 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.

Las etapas de ejecución de la auditoría son las siguientes:

- Reunión inicial.
- La recogida de evidencias, que se realiza mediante cuatro estrategias:
    - Análisis de documentación aportada por la auditada.
    - Comprobación de registros.
    - Inspección visual de los sistemas de la información y entorno físico.
    - Entrevistas con el personal, tanto Responsable/s de Seguridad como diversos usuarios.
- Documentación de los resultados.
- Reunión final para comentario de las evidencias con el Responsable de Seguridad de la auditada.
- Elaboración del informe de auditoría.

9.2 Procedimientos de notificación y gestión de incidencias.

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.

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.”

Finalmente, el informe de auditoría debe contener:

1. Objetivo de la auditoría.
2. Identificación de los auditores.
3. Personas contactadas.
4. Fecha de la auditoría.
5. Normas de referencia.

6. Descripción de las no conformidades encontradas, y la toma de las acciones correctivas.
7. Eficacia del sistema para el cumplimiento de los requisitos de la norma y documentos.
8. Lista de distribución del informe.
9. Adjuntar observaciones y recomendaciones para adecuar la empresa a la protección de datos

Las incidencias se deben notificar y almacenar en un registro siguiendo el siguiente formato:

- Tipo de incidencia
- Fecha de la incidencia o de su notificación
- Persona que ha notificado esta incidencia
- A quién se escala la incidencia
- Qué efectos se han producido
- Qué medidas correctoras se han puesto en marcha

9.3 Control de los registros de sistemas de seguridad

El objetivo del control de registro de seguridad consiste en chequear si la información se encuentra segura, todo esto es con el fin de evitar la filtración de información que puede ser en extremo relevante (como es el caso de cuentas bancarias, DNI, etc.) para esto se utilizan los siguientes criterios:

- Registro de calidad
- Identificación
- Almacenamiento
- Protección
- Recuperación
- Retención
- Disposición de los registros

Todos estos criterios son analizados con el fin de buscar si alguno de estos está fallando y si se puede mejorar en el menor tiempo posible

9.4 Auditorías (internas y externas)

Para iniciar, las auditorías LOPD consiste en una herramienta la cual se utiliza para conocer todos los fallos y oportunidades de mejora que puede tener una aplicación o autómata, esto se logra mediante la investigación, revisión, consulta, comprobación y obtención de toda la evidencia sobre un hecho o sistema establecido, todo esto con el fin de poder garantizar las medidas de seguridad para evitar la filtración de información personal (todas las obligaciones se encuentran en el decreto real 1720/2007 del 21 de diciembre en el que se aprobó el reglamento de desarrollo de la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal, que se establece en su artículo 96). Para esto existen 2 tipos de auditorías:

- Auditorías Externas: estas son realizadas por un especialista en la materia el cual no tiene ninguna relación con la compañía que será auditada, para esto realiza las técnicas mencionadas anteriormente, todo esto con el fin de poder garantizar la seguridad y fiabilidad del sistema de seguridad. En estas auditorías la relación que existe entre la empresa auditada y el auditor es del tipo civil-contractual, la cual se clasifica como una del tipo de prestación de servicios, entre 2 entes distintos.

- Auditorías internas: estas son realizadas por funcionarios internos de la compañía con el objetivo de encontrar los errores que pueden tener los sistemas de seguridad al igual que la auditoría externa, a diferencia de la externa, la relación entre el auditor y la empresa auditada es de subordinación y dependencia, dado que este tiene una relación contractual directa con la compañía.

Los procesos para realizar una auditoría son(ya sea interna o externa):

- Organización e inicio: aquí es donde se fijan los objetivos de la auditoria, todo esto en términos de fijar cuáles serán las medidas y controles a utilizar (las cuales se deben apegar a la ley). Debemos también establecer el alcance de la auditoría, es decir, los trabajos a realizar, y responsables para realizarlos.
- Planificación y toma de datos: en esta parte se realiza un calendario a seguir, en el cual se detallan las entrevistas, los plazos para obtener los documentos necesarios para la recogida de datos y la documentación de las bases del proyecto. Posterior a esto se estudia toda la información recopilada y se realiza un informe de la toma de datos.
- Verificar cumplimientos: Realizar las verificaciones, mediciones y controles necesarios y contrastarlo con la información y documentación obtenida.
- Informe final: en esta parte se Identifican los incumplimientos, deficiencias y aspectos a mejorar, valorar el grado de adecuación de las medidas y controles existentes a la ley. Además de esto se realizan las conclusiones y se proponen medidas para corregir o se sugieren ideas complementarias necesarias para evitar las fallas de seguridad. Tras todo esto, se elabora y presenta el informe de auditoría y el informe ejecutivo para la Dirección con los resultados más relevantes obtenidos.

10 Referencias y bibliografía

La información se ha extraído principalmente de las webs oficiales de la AEPD y de los artículos de la LOPD que se encuentran en la web del BOE:

- Agencia Española de Protección de Datos: http://www.agpd.es
- Boletín Oficial del Estado: http://www.boe.es

A continuación, citamos otras referencias específicas de cada punto (donde procede).

10.1 La AEPD

- https://es.wikipedia.org/wiki/Agencia_Espa%C3%B1ola_de_Protecci%C3%B3n_de_Datos
- http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php

10.2 Registro de ficheros

- http://www.cuidatusdatos.com/infoformularionota.html
- https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/inscripcion_ficheros/index-ides-idphp.php
- http://www.agpd.es/portalwebAGPD/ficheros_inscritos/estadisticas/index-ides-idphp.php
- http://www.bloguismo.com/inscribir-ficheros-agencia-proteccion-datos/

10.3 Seguimiento y control (Auditoría LOPD)

- http://zugastiabogados.es/cuando-y-como-hay-que-realizar-una-auditoria-en-lopd/
- https://www.audisec.es/es/auditoria-lopd/
- https://www.josemanuelsanz.es/lopd-practica-el-registro-de-incidencias/